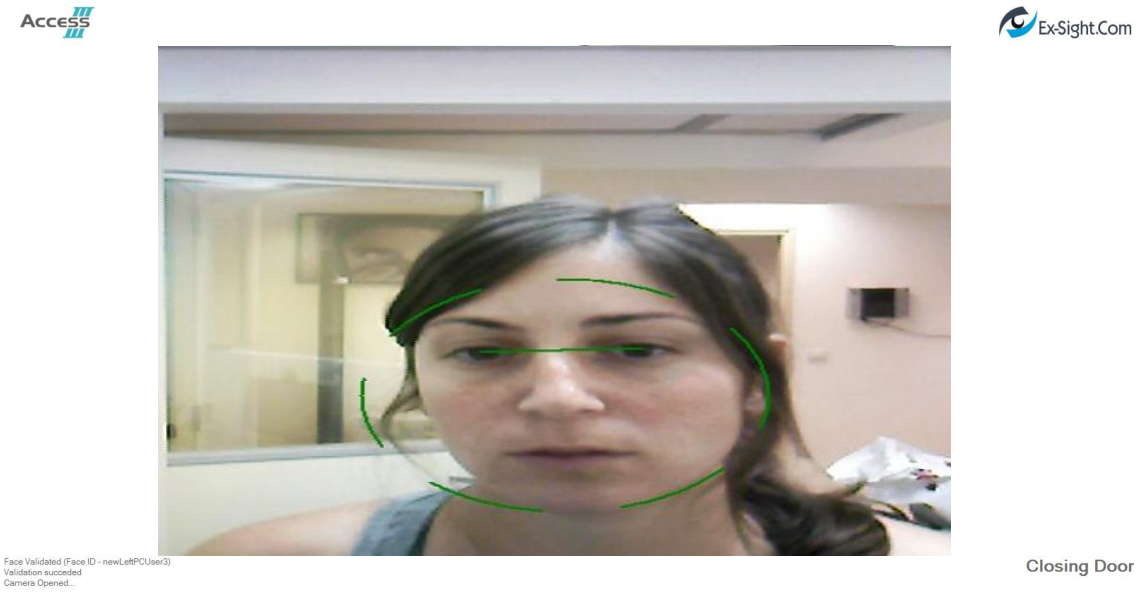
Ex-Sight.Com
ACCESS*III*
User Manual

Last Update: 13/12/2010



Contents

1 Overview 5

1.1 Software Screenshot 5

1.2 Special Features 5

1.3 Software Specifications 5

1.4 User Interface 6

1.5 Supported Cameras 6

1.6 Database 6

1.7 Facial Recognition Settings 6

1.8 I/O 7

1.9 Speech 7

1.10 Network 7

1.11 Operating Systems 7

2 Limitations 7

2.1 Environment 7

2.2 Pose 7

2.3 Face Condition 7

2.4 Eyeglasses 7

2.5 Identification distance 8

3 Hardware Components: 8

3.1 Door Alert Connection Diagram: 8

The Door Alert option allows real-time detection of door break. 8

3.2 Minimal PC Requirements: 9

3.3 Face Tracking: 9

4 AccessIII Installation: 10

4.1 AccessIII Registration: 12

4.1.1 Manual Registration: 12

4.1.2 Online Registration (Requires internet connection): 13
4.2 Physical Installation 13
5 ACCESS III QUICK START GUIDE 14
5.1 Device Installation Locations 14
5.1.1 Recommended Locations 14
5.2 Software Usage Recommendations 14
5.2.1 Recommended distance from Access III Device 14
5.2.2 Recommended Facial Position 15
5.2.3 Face Enrollment 15
5.2.4 Enrollment and Verification 15
6 Application: 16
6.1 Creating Administrator: 16
6.2 Application Tabs: 18
6.2.1 Video Tab: 18
Administrator Access: 18
Admin Mode - Settings Tab: 19
6.2.1.1 Factory Settings button: 21
6.2.1.2 Camera Settings button: 21
6.2.1.3 Replication: 22
6.2.1.4 Web Interface: 22
6.2.1.5 Attach User's Picture: 22
6.3 User Management Tab: 23
6.3.1 Adding Users: 23
6.3.2 Deleting users: 25
6.3.3 Adding and Validating Fingerprints: 26
6.3.4 Searching for users in the local database: 27
6.3.5 Adding templates to a selected user: 27
6.4 Opening gate/door: 27
6.5 Timezone Tab: 28
6.5.1 Creating a Primary Time zone: 28

6.5.2 Adding a def Time zone: 29
6.5.3 Deleting Time zone: 29
6.6 Group Tab: 30
6.6.1 Creating a group: 31
6.6.2 Deleting a group: 32
6.7 Shutdown Tab: 32
AccessIII Web Interface: **33**
6.8 Users List: 33
6.9 Log Entry: 34
6.10 Validated Users: 35
6.11 Rejected Users: 36
6.12 Entry counter: 37
6.13 Entry Hours: Calculating working hours 38
6.14 Realtime View: 39
6.15 Diagnostic Page: 39
Change List: **40**

1 Overview

ACCESSIII is cutting-edge physical access control software with high accuracy and unique features:

Face Recognition Capabilities:

- Constant Face Detection (1:N Mode)
- Multi Modal Verification (1:1 Mode)
- Supporting: RFID, Code, Magnetic Card
- Liveness Tests – Verifies the video is based on live feed and not a picture
- Face Quality Filter – Defines the minimum image quality needed for Verification/Enrollment
- Ageing – Automatic Face Adjustment

Access Control Features:

- Users / Time Zones Management
- Entry Counting / Tracking
- Group Access
- Task-Entry Reporting

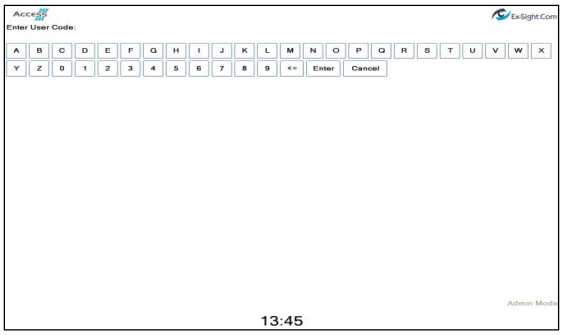
Networking:

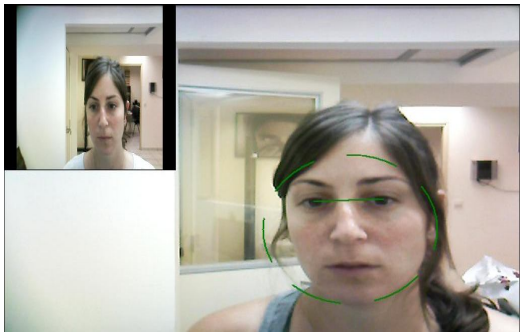
- Database Replication
- Flexible Database Location
- Internal Web interface

Video:

- DirectX / Win32API support
- IP CAMERAS (MPEG4 / H.264)

1.1 Software Screenshot





1.2 Special Features

1:1 / 1:N Detection
Individual / Group Detection
Fingerprint / FACE / RFID / CODE / MAGNETIC Support
Entry Counting
Dual Face Algorithm

1.3 Software Specifications

Web interface
Facial Recognition customizable engine

Generic / IP video interface
Real time facial detection
Real time facial matching
Enhanced matching mechanism (Matching attempts)
Adjustable image processing
User Management / Time Zones
Time Attendance feature (In / Out) (Reasons)
Fully customable Time Attendance
Remote door opening (Up to 4 doors in standalone version)
Log Browser including visual history
User Privacy mode – no image saving
Silent Alarm when user is not authorized
Automatic suspect capture

1.4 User Interface

Visual view of video input
Visual view of face detection
History / Enrolled / Suspects view
Voice alerts during system operation
Do-it-yourself localization available
Easy to use graphic interface
Touch Input Interface

1.5 Supported Cameras

Full support for Analogue cameras through video grabber
Full support for USB cameras
H.264/MPEG4 for IP Cameras

1.6 Database

Microsoft Jet 4.0
Networked / Standalone
Dynamic location of database
Integral Import/Export feature
Web reporting mechanism
Unlimited number of users
Optional Database customization to customer's needs

1.7 Facial Recognition Settings

Aging Minimal Threshold
Allow Aging
Allow Liveness
Face Confidence Threshold
Face Quality Threshold
Liveness Threshold
Matching Attempts
Matching Threshold
Maximal IOD
Minimal IOD
Number Of Frames For Enrolment
Number Of Frames For Validation
Camera

Camera Type
Frame Rate
Rotate
Video Format

1.8 I/O

DIO card with 4 Relays 240VAC/10A
Optional: Inner Camera I/O

1.9 Speech

Speech alerts for access events

1.10 Network

Software database can be shared on Network
Remote control through web

1.11 Operating Systems

Windows XP, Vista, 7

2 Limitations

2.1 Environment

- FRS algorithm should be used in constant lighting conditions for best performance.
- It is recommended to use two templates: Day & Night.
- Lighting must be equally distributed on each side of the face and from top to bottom.
- There should be no significant direction of the light or visible shadows.
- Care must be taken to avoid "hot spots". These artefacts are typically caused when one, high intensity, focussed light source is used for illumination.

2.2 Pose

Frontal Pose: ±15 degrees from frontal in every direction

2.3 Face Condition

Beard, moustache and other changeable face features sometimes influence face recognition similarity level. If you want better performance, please include face with beard and cleanly shaved face enrolled with identical ID.

2.4 Eyeglasses

There should be no lighting artefacts on eyeglasses. This can typically be achieved by increasing the angle between the lighting, subject and camera to 45 degrees or more. If lighting reflections cannot be removed, then the glasses themselves should be removed. (However this is not recommended as face recognition typically works best when matching people with eyeglasses against themselves wearing

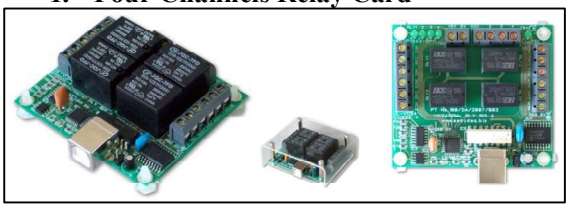
the same eyeglasses). Glasses have to be of clear glass and transparent so the eyes and irises are clearly visible. Heavily tinted glasses are not acceptable.

2.5 *Identification distance*

Identification distance is not limited while the image quality remains. The face will be recognized only if the minimal distance between two eyes will be at least 40 pixels. For example, 10 X Zoom camera within the distance of 25m from the subject, works.

3 ***Hardware Components:***

1. **Four Channels Relay Card**



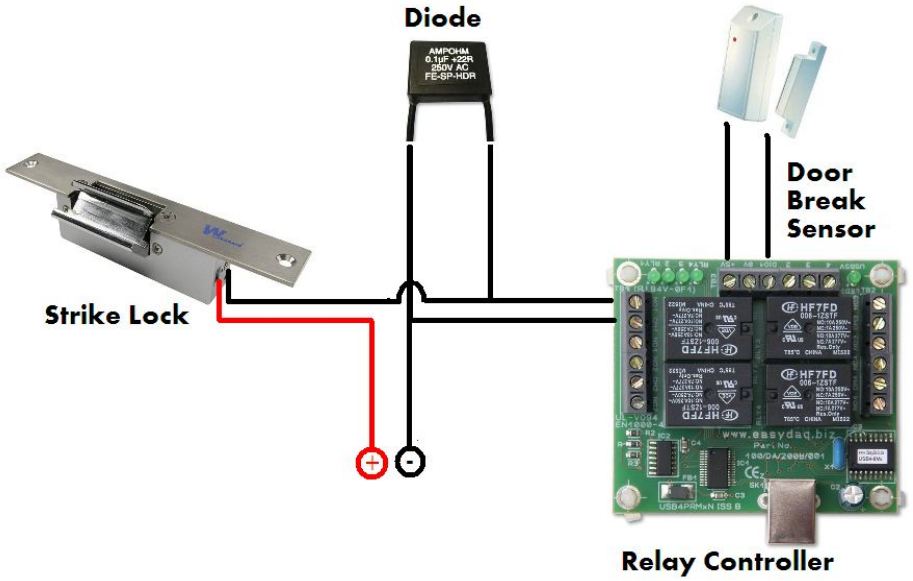
2. **NIR (Near Infra Red) USB Camera**

3.1 *Door Alert Connection Diagram:*

The Door Alert option allows real-time detection of door break.
Using a standard door sensor along with "Door Alert" option enabled, allows detection of unauthorized door entry.

Door Sample Rate – Door Sample Rate is the time between door status check.The samples, taken to check whether the door has been illegally opened.
Enable Alert – "True" = Alarm is enabled. "False" = Alarm is disabled.

To enable this option, go to - > "Settings Tab" - > Door Control Setting - > Enable Alert and change its status to "Enable".
In order to allow zero magnetic interference it is recommended to connect the Relay controller with the following Diode. This is a Connectivity Diagram of Relay Controller with AC power source and the Diode.

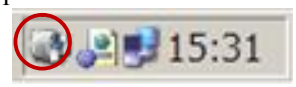


3.2 *Minimal PC Requirements:*

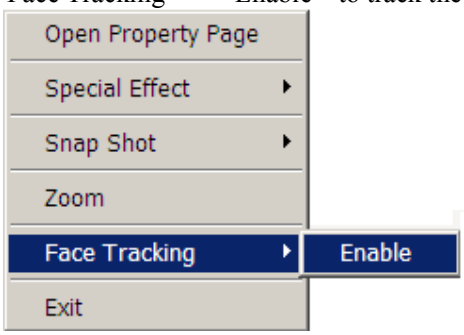
Pentium IV 1.66GHZ
512MB RAM (Minimal)
20GB Free HD
USB 2.0
Microsoft Windows XP/Vista

3.3 *Face Tracking:*

The camera is able to track the face. If this setting is enabled, the validation will be much more accurate. This option is advisable.
Optional:
To change the settings of the web camera right click this icon, located on the bottom panel of your desktop.



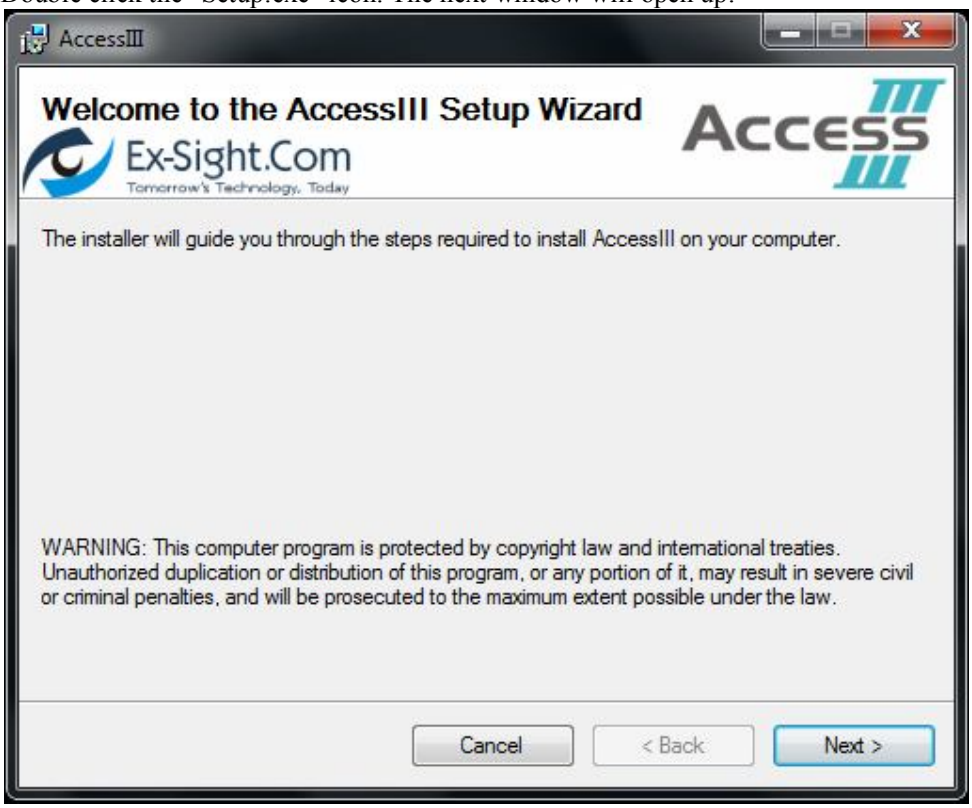
Select “Face Tracking” -> “Enable” to track the face .



The camera locates a face and zooms in on it.

4 *AccessIII Installation:*

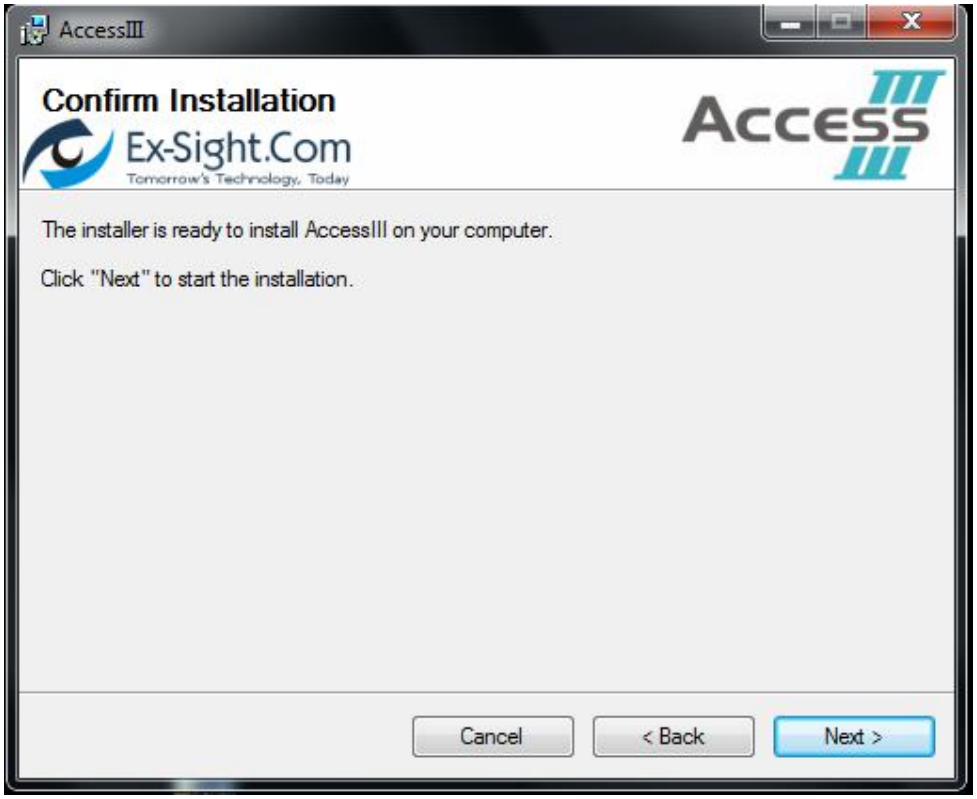
Double click the “Setup.exe” icon. The next window will open up:


AccessIII
Welcome to the AccessIII Setup Wizard
Ex-Sight.Com
Tomorrow's Technology, Today
Access III
The installer will guide you through the steps required to install AccessIII on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

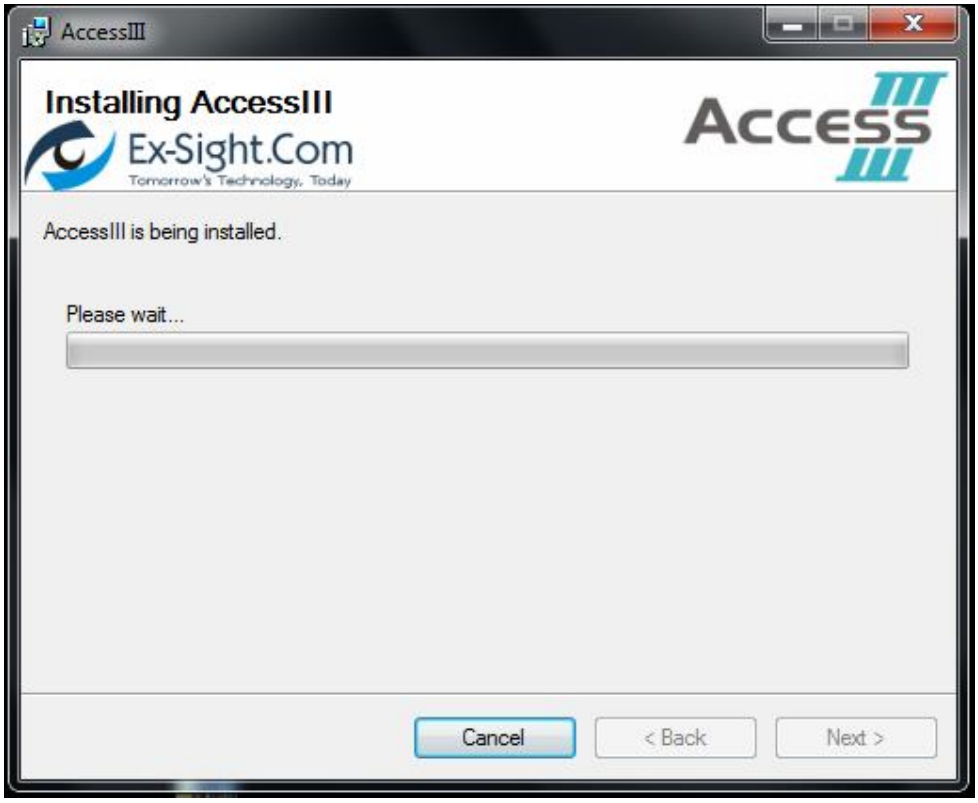
Click “Next” to continue

AccessIII
License Agreement
Ex-Sight.Com
Tomorrow's Technology, Today
Access III
Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".
EX-SIGHT.COM LTD® FRS™ ACCESS - Software License Agreement
THIS SOFTWARE LICENSE AGREEMENT (THE “LICENSE”) IS A LEGAL AGREEMENT BETWEEN “EX-SIGHT.COM LTD” AND YOU (EITHER AN INDIVIDUAL OR AN ENTITY). BY CLICKING THE “ACCEPT” BOX OR BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU REPRESENT (I) THAT YOU HAVE BEEN AUTHORIZED TO
I Do Not Agree
I Agree
Cancel
< Back
Next >

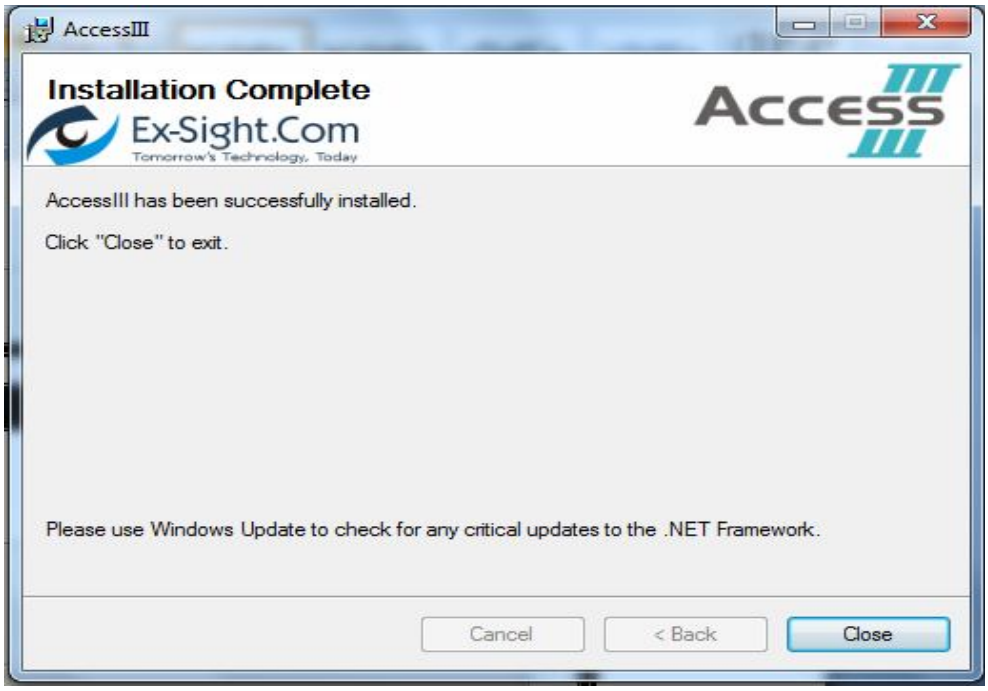
Choose the “I Agree” radio box, “Next” will be enabled. Click “Next” to continue



Click “Next” to continue



The installation is finished. Click “Close” to close this window.



4.1 AccessIII Registration:

Migration of AccessII to AccessIII:

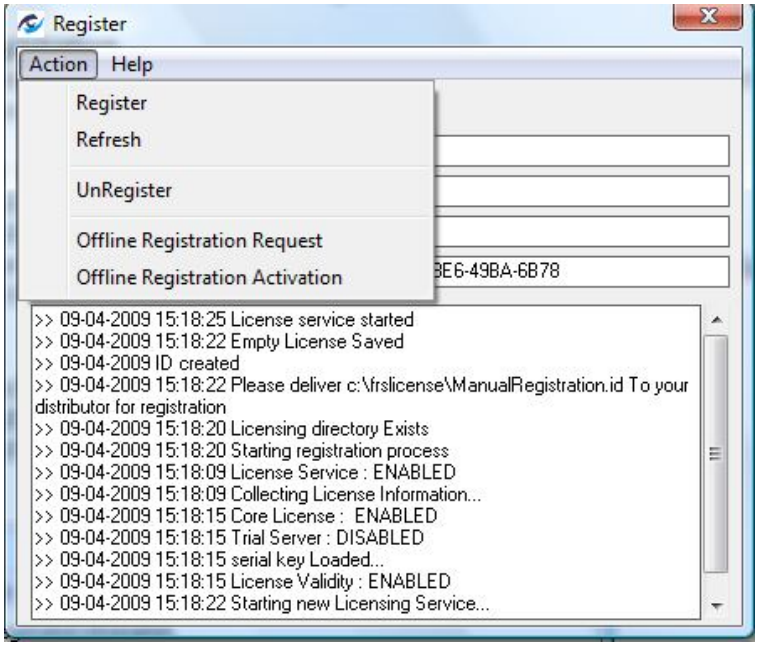
1. Deactivate AccessII license according to AccessII Manual
2. Uninstall AccessII
3. Send Ex-Sight.Com “C:\FRSLicense” Directory (Support@Ex-Sight.com)

Launch the registration application located on your desktop:

4.1.1 Manual Registration:

Manual registration allows users that do not have direct internet connection on their PCs to use offline registration mechanism.

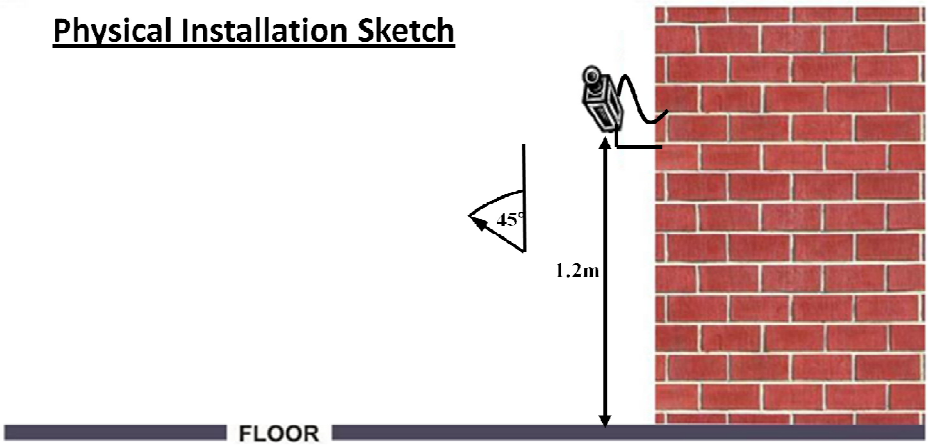
1. Enter all fields in a valid way to the registration application
2. Select "Action" Menu
3. Select "Offline Registration Request"
4. Under c:\FRSLicense\ directory you can find a file named "ManualRegistration.id"
5. Send the file to your distributor and wait for 2 files:
    a. Serial.id
    b. FACEPORT.LIC
6. Copy the files to "C:\FRSLicense\"
7. Select "Action" menu
8. Select "Offline Registration Activation"


Register
Action
Help
Register
Refresh
UnRegister
Offline Registration Request
Offline Registration Activation
BE6-49BA-6B78
>> 09-04-2009 15:18:25 License service started
>> 09-04-2009 15:18:22 Empty License Saved
>> 09-04-2009 ID created
>> 09-04-2009 15:18:22 Please deliver c:\frslicense\ManualRegistration.id To your distributor for registration
>> 09-04-2009 15:18:20 Licensing directory Exists
>> 09-04-2009 15:18:20 Starting registration process
>> 09-04-2009 15:18:09 License Service : ENABLED
>> 09-04-2009 15:18:09 Collecting License Information...
>> 09-04-2009 15:18:15 Core License : ENABLED
>> 09-04-2009 15:18:15 Trial Server : DISABLED
>> 09-04-2009 15:18:15 serial key Loaded...
>> 09-04-2009 15:18:15 License Validity : ENABLED
>> 09-04-2009 15:18:22 Starting new Licensing Service...

4.1.2 Online Registration (Requires internet connection):

1. Enter all fields in a valid manner to the registration application
2. Select "Action" Menu
3. Select "Register" option
4. Wait for registration confirmation
5. If registration process fails please contact your distributor

4.2 Physical Installation



5 ACCESS III QUICK START GUIDE

5.1 Device Installation Locations

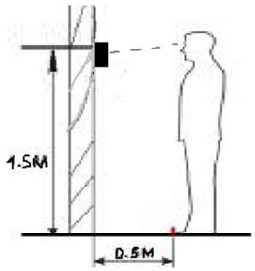
5.1.1 Recommended Locations

Outdoors	Indoors
no direct sunlight	not too close to a light source

5.2 Software Usage Recommendations

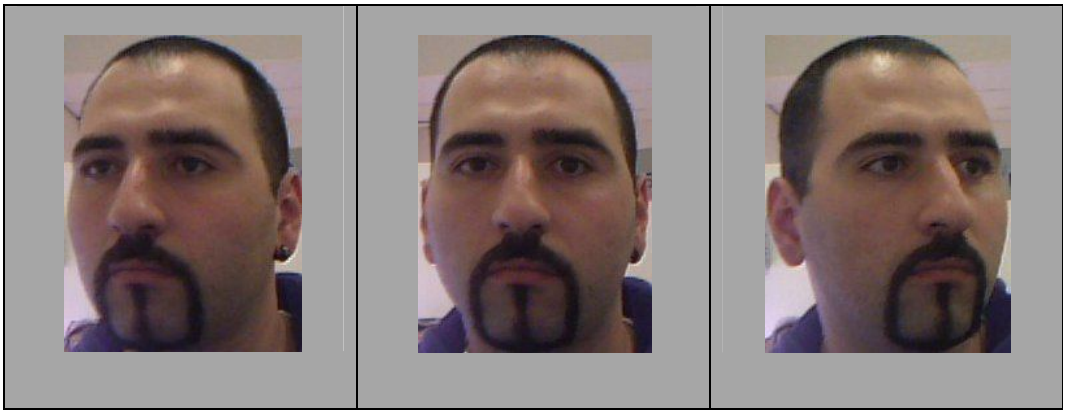
5.2.1 Recommended distance from Access III Device

For users 5-6 feet tall (1.5m – 1.9m) the recommended standing distance is about 2 feet (0.5m) from the device.

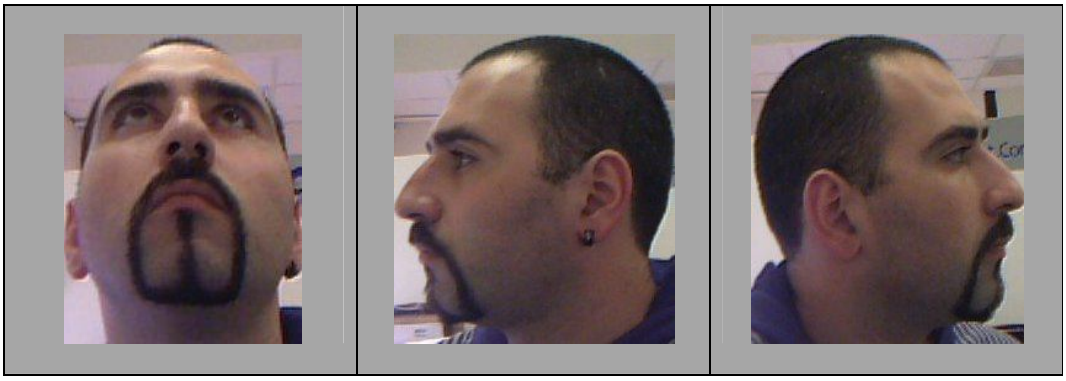


5.2.2 *Recommended Facial Position*

Recommended face position



Not Recommended face position



5.2.3 *Face Enrollment*

During the Enrollment process, position your face in front of the camera in the device.
While looking ahead at the camera, move your face slowly a few inches to each side.

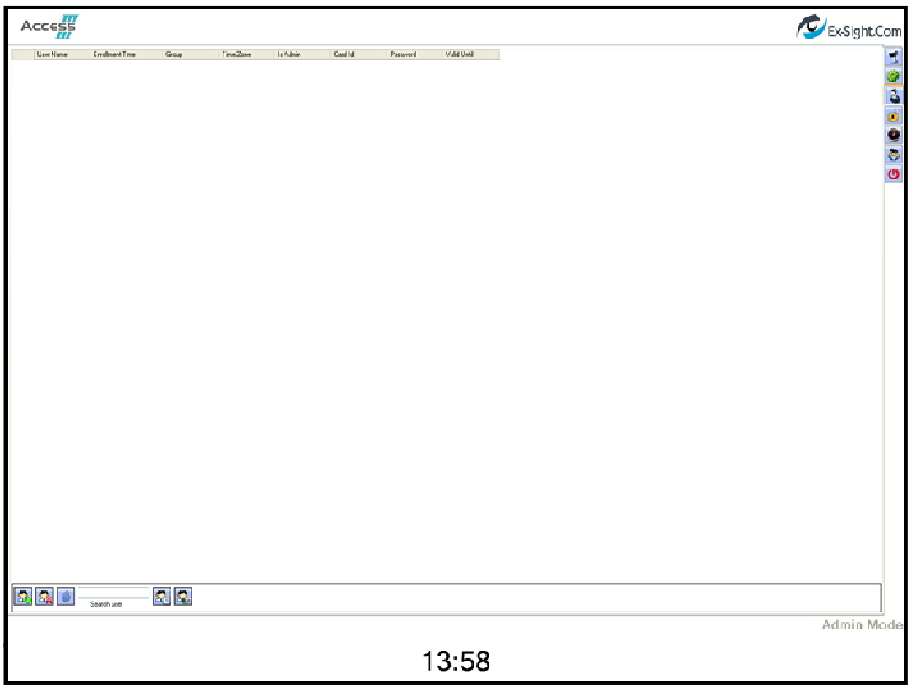
5.2.4 *Enrollment and Verification*

1. Access III Identity Enrollment is done with the objects Face Enrollment,
2. While the Administrator can also access the system with his\her unique password.
3. Access III has several ways of Identification and Verification:
   - 1 : N – The process is done on objects face for multiple faces located in the Data Base.
   - 1 : 1 – The process is done on objects face for one unique record, which is located by the objects name.

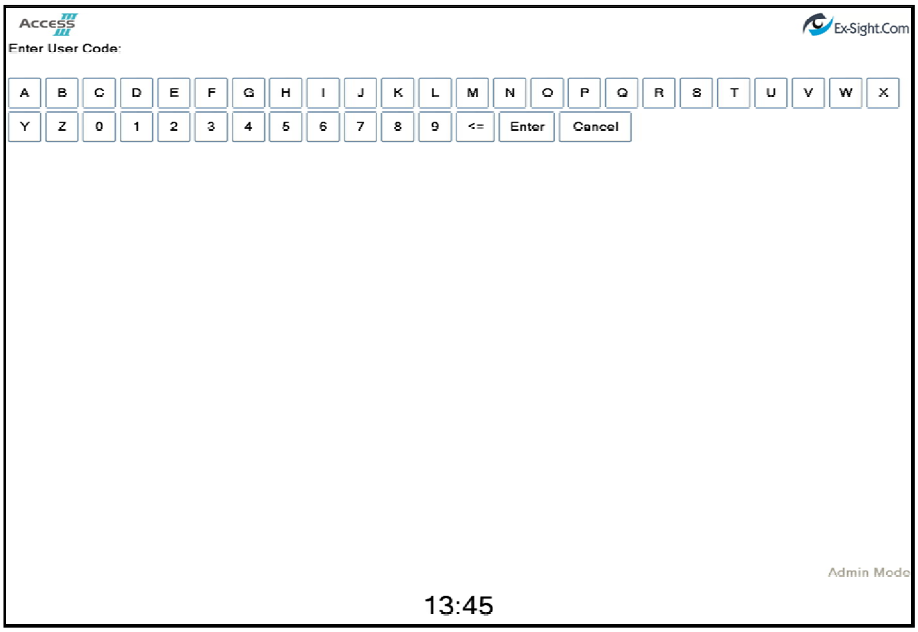
6 Application:

6.1 Creating Administrator:

After running the application for the first time, an admin user is needed to be created in order for the application to begin the video face analysis.
Run the application:



Click the “Add” button to create a new user. The next window will open.



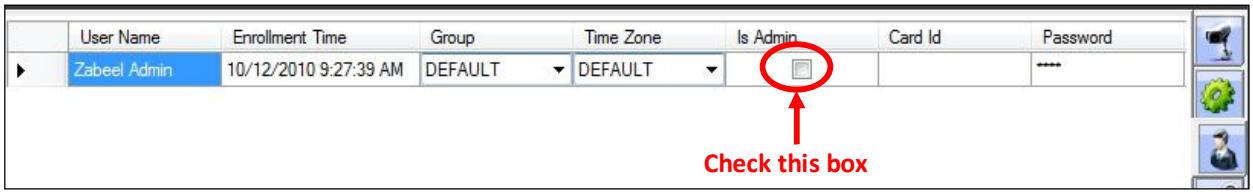
Enter the user name and click “Enter”.

At this stage the camera will scan your face and enter the images into its database.

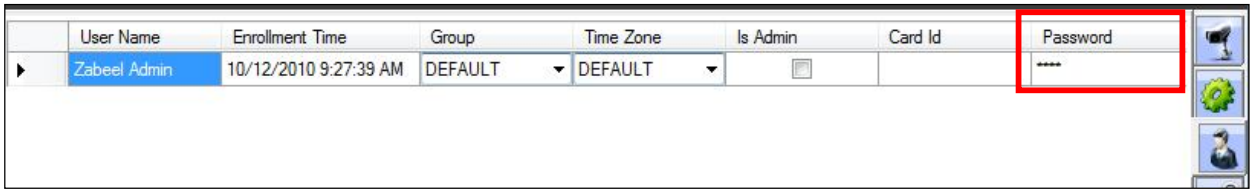
The number of images, for validating a face can be changed at:
Settings tab -> NumberOfFramesForEnrollment. Recommended: 5. The higher the number of frames, the higher the percentage of validation success.

After the camera finishes scanning your face, your user name will be added to the users list. If you wish to be the admin of the system, check the admin checkbox.

If an admin user does not exist in the system, the face validation mode cannot be started.



Optional: A password can be assigned for the administrator.



Optional: A password can be assigned for administrator.

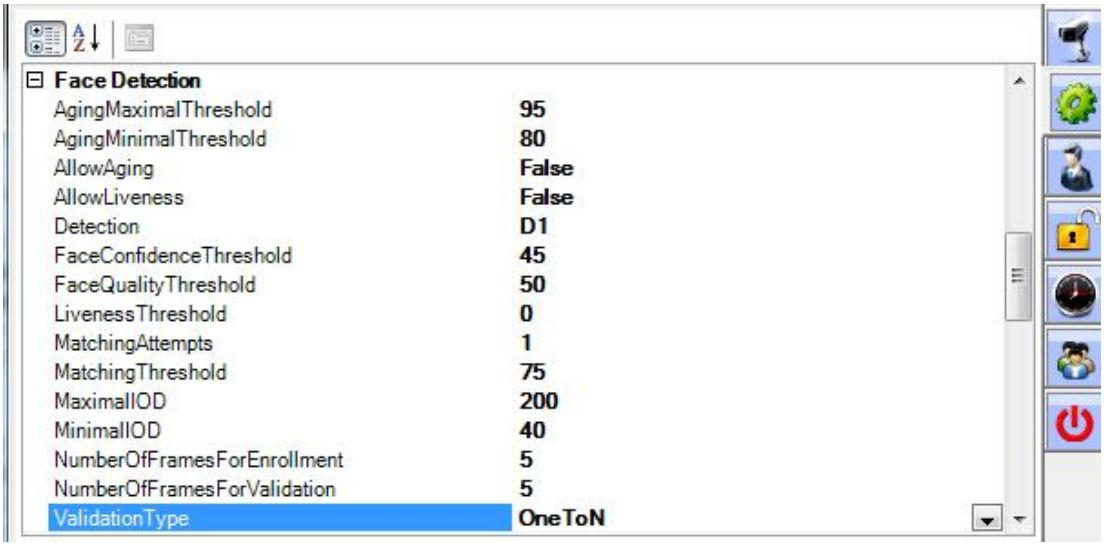
Admin password allows facial validation bypass. You can use it by clicking the "ACCESSIII" logo during validation process.

6.2 *Application Tabs:*

6.2.1 *Video Tab:*

Clicking the Video tab will start the face validation mode. This mode can be started only if a user, which has been set as administrator, is created.

Two types of Validation Type exist: 1:1 and 1:N. Validation Type can be set at:
Settings tab -> Validation Type.



- **OneToOne** – To open the gate, the user has to provide user name or Card swipe previously to
- face verification. If the username / card are valid, the system will start the face validation process.
- **OneToN** - To open the gate, the user needs to stand in front of the camera. The validation process will start automatically.

If "Fingerprint Settings" -> "allow fingerprint" is set to "True", the OneToN and the OneToOne are disabled and the validation process is as described: first fingerprint is validated and then the face is attached to the fingerprint.

Performance Differences:
There is a big difference between One to One verification to One to N identification. One to One is faster and more secured. It is not recommended to use One To N with more than 100 users in the database.

Administrator Access:

After starting the Validation mode, entering into system settings etc (only admin user can enter this state), can be done in two ways:

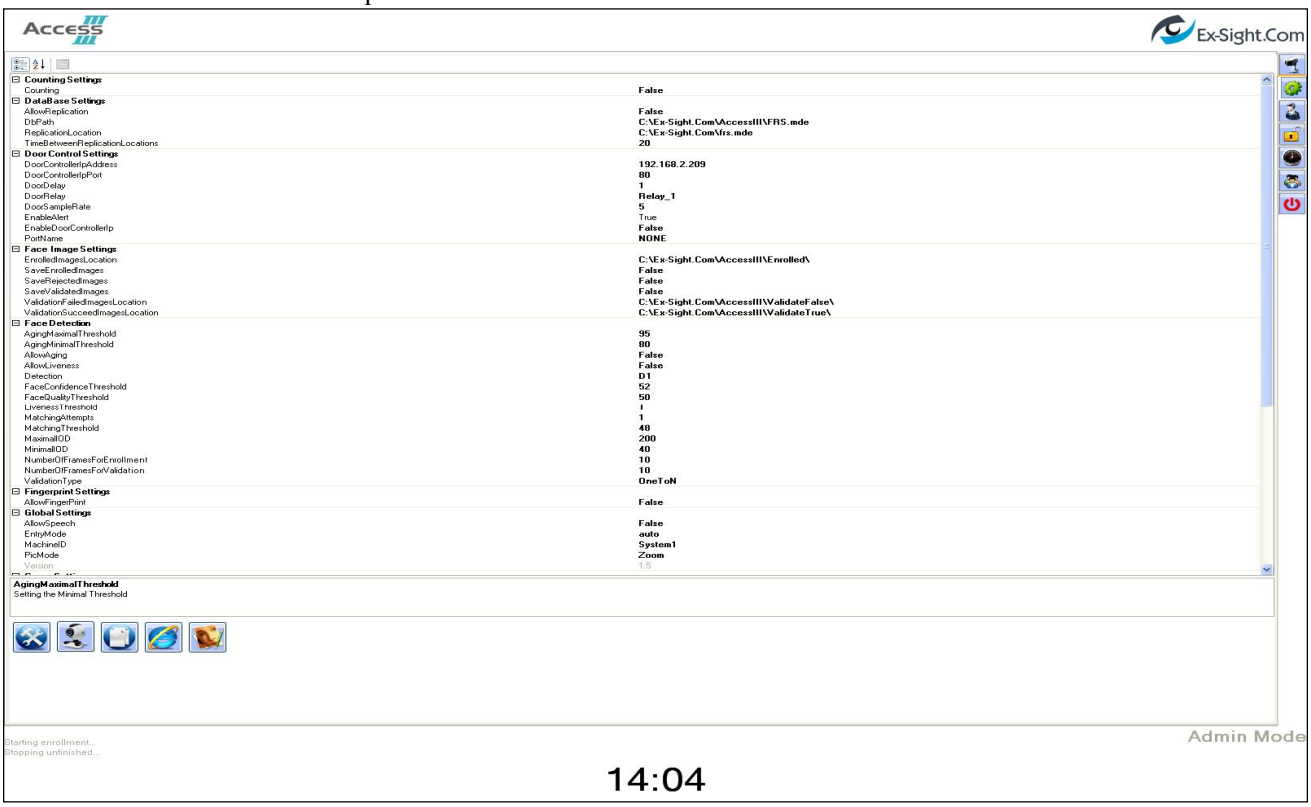
1. If a password was made, click the Ex-Sight logo.
   A window, requesting a password will open. Enter administrator's password and click "Enter". The system will transfer you to User Management tab.

2. Otherwise, at the moment the system validates your face and welcomes you, right click the mouse or press extensively (for few seconds) on the touch screen. The system will transfer you to User Management tab.

Admin Mode - Settings Tab:

To enter the settings, click the settings tab:

The next window will open:



Counting Settings:

Counting – Limits the user access according to daily Time zone counter.

Data Base Settings:

Replication allows reliable synchronization between similar databases, such as Client-Server. Below you can find the parameters that affect the synchronization process.

Allow Replication – "True" = allows synchronization between AccessIII client db ("C:\Ex-Sight.Com\AccessIII\FRS.MDB) to the specified database under the same name in the **ReplicationLocation** directory. "False" = no replication is done.
Replication Location – The target directory location for FRS.mdb File.
Time Between Replications – Time, in minutes, between each replication.
Recommended Value: 60.

Door Control Settings:
Door Delay –Delay time the gate/door will remain open.
Door Relay – The relay to which the door is set to.
Door Sample Rate – Recommended value: 5 sec. If "Enable Alert" is set to "True", Door Sample Rate is the time between door status check. The samples, taken to check whether the door has been illegally opened.
Enable Alert – "True" = Alarm is enabled. "False" = Alarm is disabled.
Port Name – The port to which the door controller is connected to.

Face Image Settings:
Enrolled Images Location – Enrolled faces path.
Save Enrolled Images– "True" = Save, "False" = do not save
Save Rejected Images – "True" = Save, "False" = do not save
Save Validated Images– "True" = Save, "False" = do not save
Validation Failed Images Location – Validation failed faces path.
Validation succeeded Images Location – Validation succeeded faces path.

Face Detection:
Aging Minimal Threshold* – Minimal aging allowed. Recommended: 85.
Allow Aging* – "True"= enable allowing aging option. Recommended: false
Allow Liveness* – "True" = Checks if the user is not a static image. Recommended: false
Detection – Detection engine – (D1/ D2/ D1 and D2)
Face Confidence Threshold* – Confidence Face Detection level. How much the system is sure the image looks like a face. Recommended: 50
Face Quality Threshold* – Face clearance. Recommended: 50
Liveness Threshold* – Setting for liveness quality threshold. Recommended: 0
Matching Attempts* – The number of times the system will try to match the face.
Recommended: 1
Matching Threshold* – The similarity lower limit of recognition . Recommended: 78
Maximal IOD* – Maximal inner ocular distance (the maximal distance between two eyes). Recommended: 200, depends on camera quality. Higher value = higher CPU consumption.
Recommended: 201
Minimal IOD* – Minimal inner ocular distance (the minimal distance between two eyes).
Recommended: 65
Number Of Frames For Enrollment* – No. of frames to process in case of enrolment.
Recommended: 10
Number Of Frames For Validation* – No. of frames to process in case of validation.
Recommended: 10
Validation Type – There can be two types of validation:

- **OneToOne** – To open the door/gate, the user first has to enter his username and only afterwards the system begins validating the users face.
- **OneToN** - To open the door/gate, the user only needs to stand in front of the camera and the system will validate the users face.

Recommended: **OneToOne**
*** The above value affects System Performance, please contact manufacturer before change of default value.**

Fingerprint Settings:
Allow Fingerprint – "True" = Fingerprint mode is enabled. This means that any other mode is disabled and replaced by this mode. The system will expect the user to place his finger, then validate user's face.

Global Settings:
Allow Speech – "True" = enable systems speech. All operations will be escorted by a voice, speaking the chosen language.

Entry Mode – It is possible to save the "direction" of users in the log, depending the mode:

- **In** – In direction will be entered to all users, all the time.
- **Out** – Out direction will be entered to all users, all the time.
- **Manual** – After the user is validated, the application asks the user to input his direction. The direction is then saved to the log.
- **ManualWithReason** – After the user is validated, the application asks the user to input his direction. If the direction is set to "Out", the application opens a combo box with reasons, from which the user can choose the reason. The direction is then saved to the log. If the direction was "Out" the reason is saved as well in the log.
- **Auto** – Each time a user is identified, the mode flips.

Language – The Language for speech and user interface. Set from the dropdown list. The administrator interface is English only.
Machine ID – Machine name.
Version– The Version of the application.

Group Settings:
Allow Group – "True"= Group mode is allowed. If numbers of users are set together in a group, only identifying all together, the system opens the door/gate.
Group Delay – Setting the delay time for all faces within a group to appear on the camera view.

RFID Control Settings:
RFID Port – RFID connection port. Can be chosen from the dropdown list.

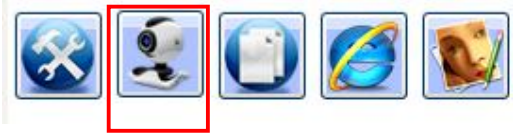
Video Settings:
Camera Type – Setting the camera type. (DirectX / Generic / IP camera).
IP camera – The source is an IP camera.
IP Address* the IP Address of the camera.
IP source Type* –The type of the camera (VACAM/ Axis/ ASONI/ Other camera/ Movie/ Other).
Protocol* – The protocol name of the IP camera's connection. (rtsp/ http).
Port Num* – The port of the camera.
Stream Name* – The stream name of the camera connection.
Frame Rate – Setting the frame rate.
Rotate – If rotation of the screen is needed, the rotation degree can be set here.

6.2.1.1 *Factory Settings button:*

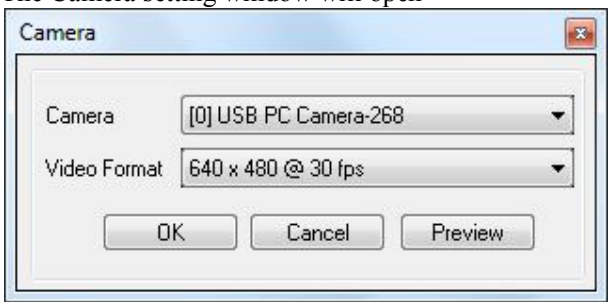
To return to the Factory settings of the system, click the recycle button in the Settings tab:

6.2.1.2 *Camera Settings button:*

To change the camera settings, click the Camera settings button in the Settings tab:



The Camera setting window will open



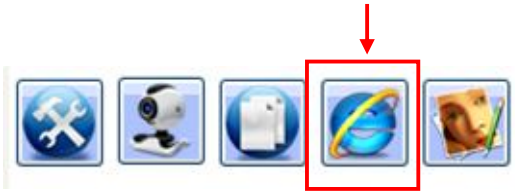
Camera – Select the camera that the system will work with (from all the cameras that are connected to the computer).
Video Format - Select the video format for the specified camera above.

6.2.1.3 Replication:

Click the Replicate button in the Settings tab to replicate the database to the pre-configured Replication Location on the settings tab:

6.2.1.4 Web Interface:

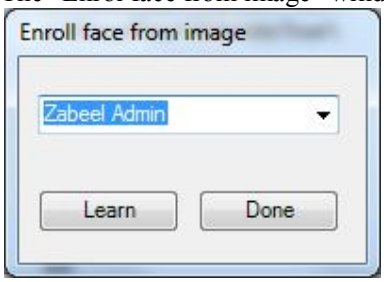
Click the internet browser button in the Settings tab in order to launch the ACCESSIII Web Interface:



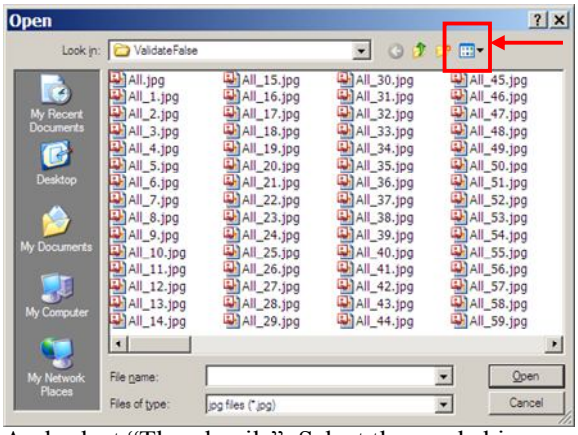
6.2.1.5 Attach User's Picture:

In order to improve the validation rate of a user, you can enroll specific images based on different sources, such as: validation failed images. These images can be attached to a certain user. This action will improve system performance on same validation conditions.
To do so, click the Attach User's Picture button in the Settings tab:

The “Enrol face from image” window will be opened:



Select the right user from the combo box and click ok to continue. The browser picture window will be opened with a default location: Validation Failed Images folder. To preview the images before selecting one, click the "views" button:



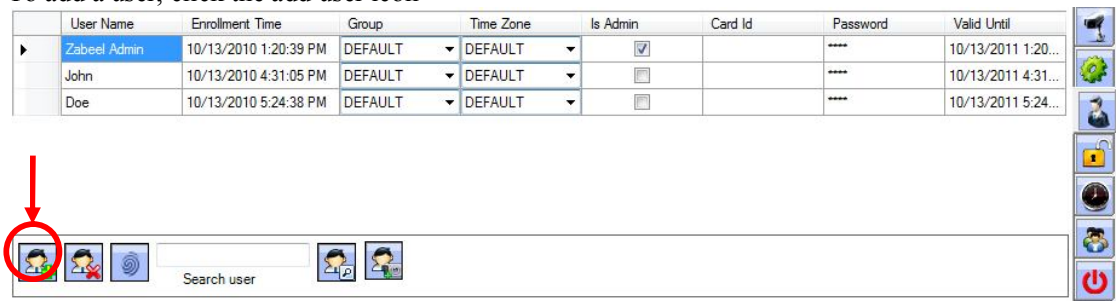
And select “Thumbnails”. Select the needed image and click “Open”. A voice will announce if validation has succeeded or failed.

6.3 User Management Tab:

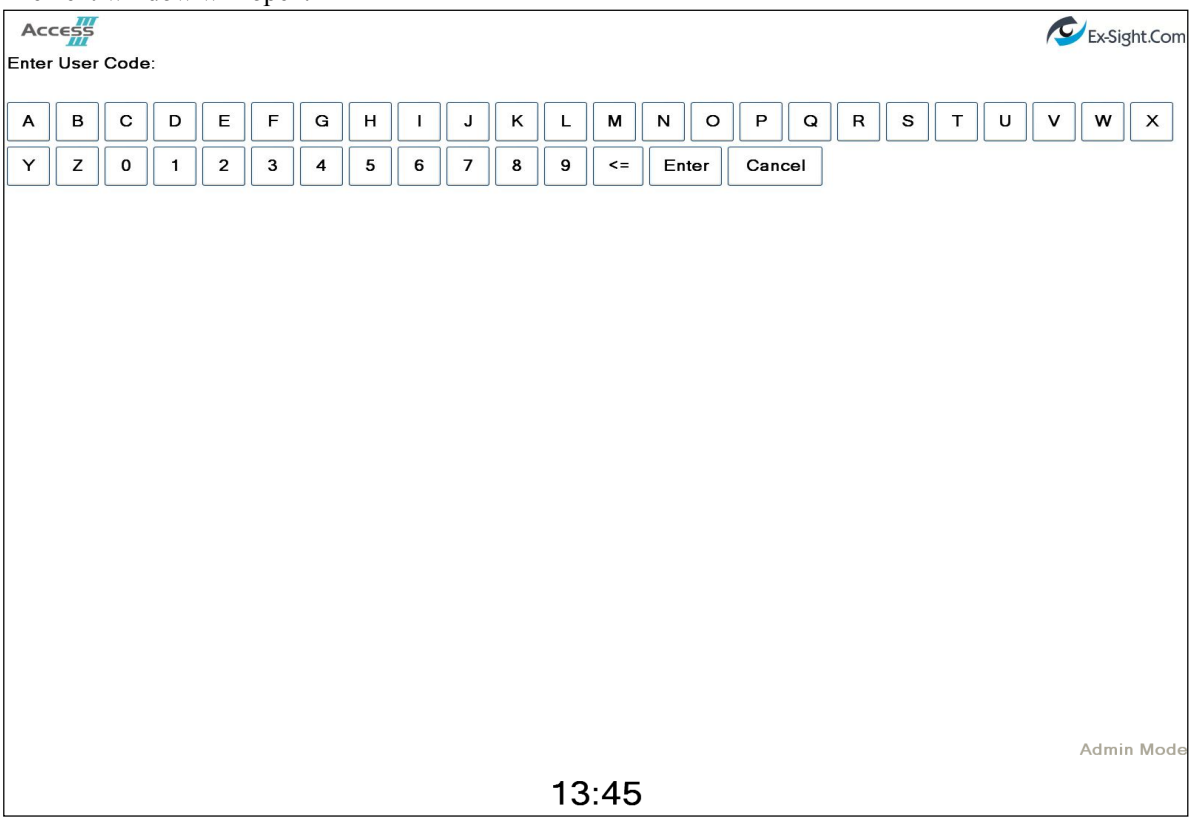
To manage users, click the User Management tab:

6.3.1 Adding Users:

To add a user, click the add user icon



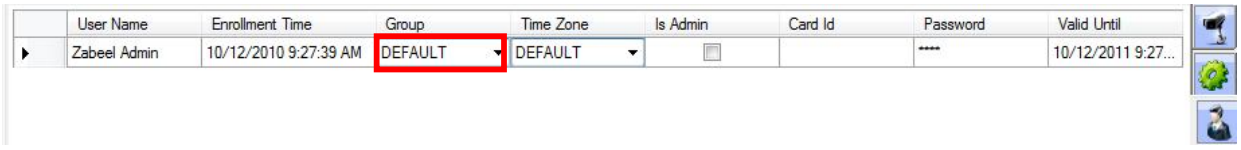
The next window will open:



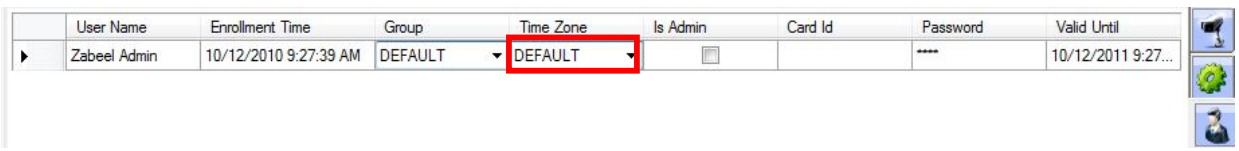
Enter the user name. User name must be longer than 2 characters. Click "Enter" to confirm the user name. The system will try to learn the face. Move your face gently from right to left / up and down, near and far from the camera. The user will appear on User Management tab if the enrollment process succeeded.

The next editing options are available for each user:

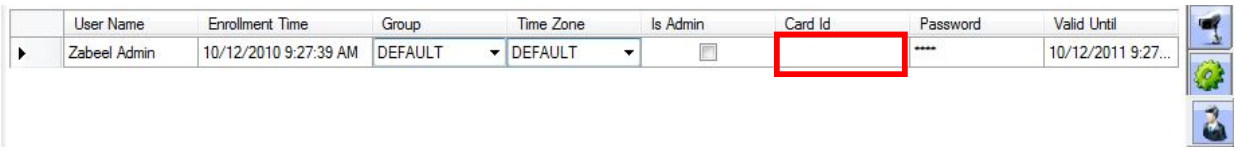
- Administrator - A user can be defined as Administrator. To do so, check the admin box (see the Creating Admin User).
- Group – In order to connect a user with a particular group: Click the dropdown group list for the user and select the relevant group.



- TimeZone – The Timezone defines the time slots the user can access the door. An already existing timezone can be set for the user. Click the dropdown list for the user and select the relevant timezone.

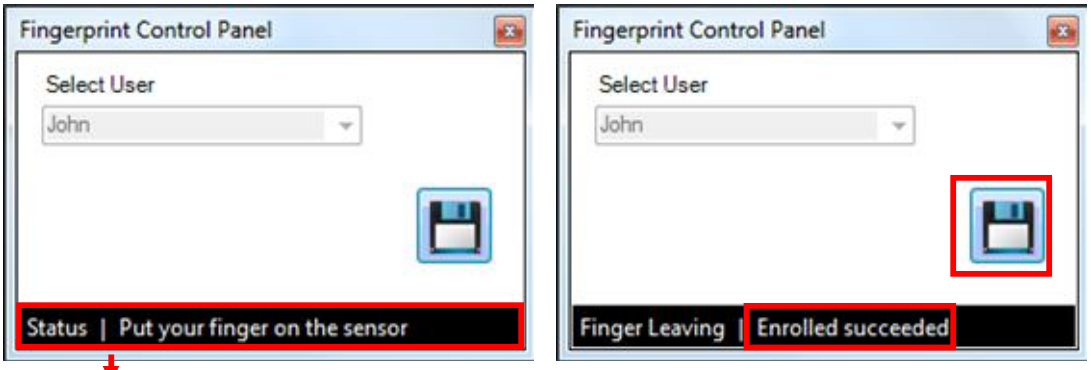


- Card ID – The Card ID is used to identify a user on OneToOne mode using a magnetic card
- or RFID. This option can be set in 3 ways:



- Manually – Click twice the Card Id field on the relevant user. Enter the number.
- Magnetic Card – Click twice the Card ID field on the relevant user. Slide the card through the card reader connected in advance.
- RFID – Click the user you want to assign the RFID number to and pass the RFID card next to the RFID card reader.
- Password – Double click the Password field on the wanted user and enter the password. Password may be used only with administrator users. The password allows clicking on the "ACCESSIII" logo and login into the system without face validation.
- Valid Until – This is the last date that the user activity will be valid. This field is set by default to a year from the moment the user is created. It is possible to change this date by clicking on and changing it.

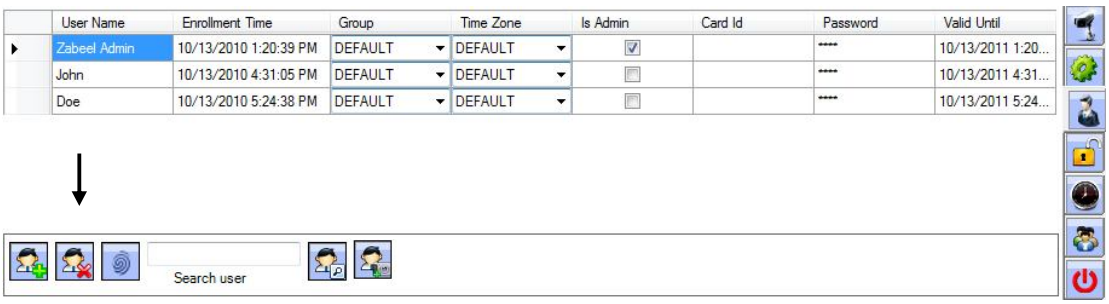
If the **"AllowFingerprint"** option is set to **"True"** in the settings tab, the next window will open:



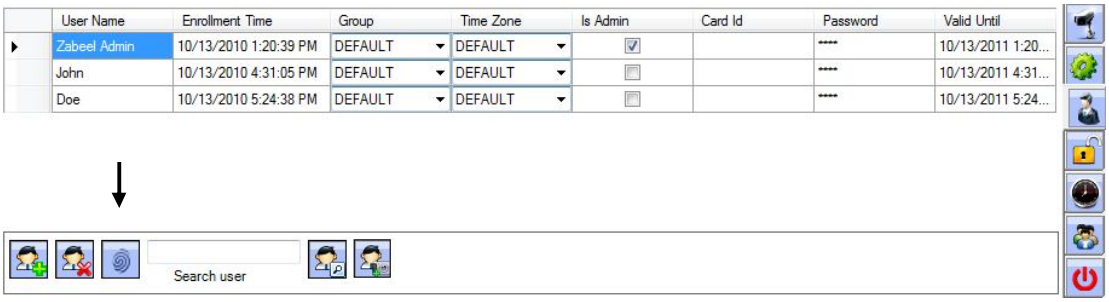
To finish adding a user, the user should place ones finger on the fingerprint reader, until **"Enrollment succeeded"** speech/status notification. Click **"Save Fingerprint and Exit"** button to finalize the user adding process.

6.3.2 Deleting users:

Click the user to be deleted from the list and click the "Delete" icon.



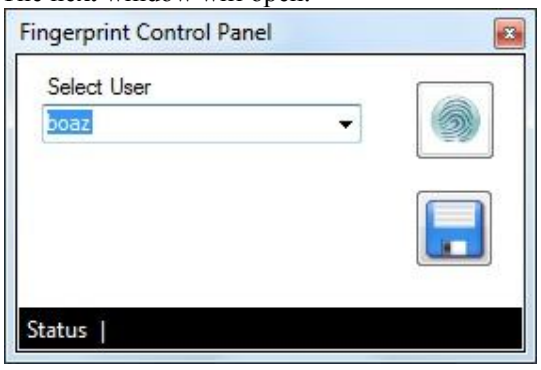
6.3.3 *Adding and Validating Fingerprints:*



In order to add a fingerprint or to set user validation mode by fingerprint, it is vital to set the "**AllowFingerprint"** option to "**True**" in the settings tab.
See **section 5.2.2 -> Fingerprint Settings**.

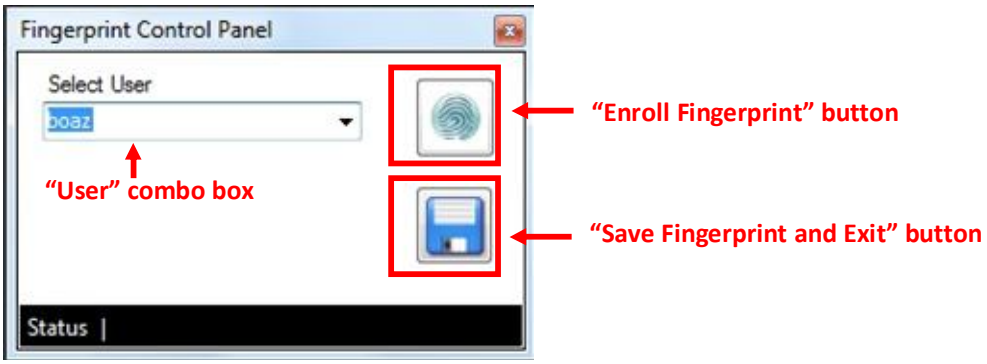
To add a fingerprint, click the "**Add Fingerprint**" icon located at the **"User Management"** tab.

The next window will open:



Validating a fingerprint:
In order to see if your fingerprint exists in software database, place your finger on the fingerprint reader until a speech/status notification sounds. If this fingerprint exists in the database, "**Validating username**" speech/status notification will sound and the Status will welcome you by your user name. If "**Validation failed**" speech/status notification sounds then your fingerprint does not exists in the database.

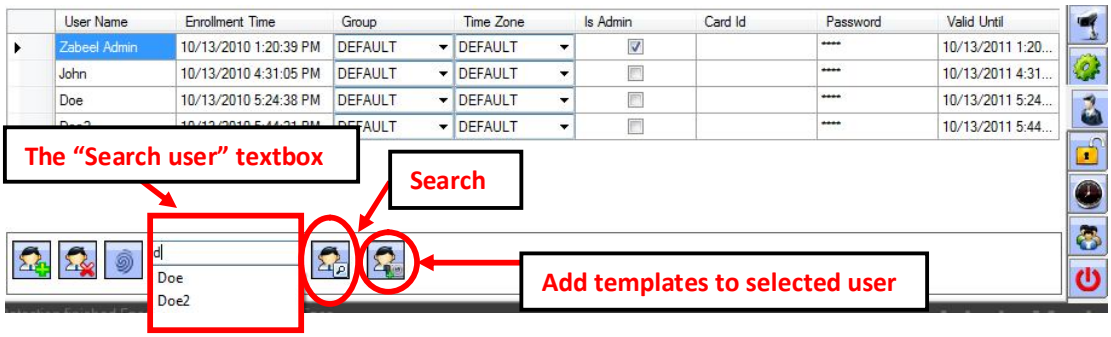
Adding new fingerprint:
Select the wanted user from "**User**" combo box and click the "**Enroll Fingerprint**" button.



Place the finger on the fingerprint reader until the "**Enrollment succeeded**" speech/status notification. Keep holding the finger down, until **"Verified user"** will sound. To save and exit click the **"Save Fingerprint and Exit"** button.

6.3.4 *Searching for users in the local database:*

Access III has the ability to search users in the local database. When the user types in letters in the "Search user" textbox, an auto-completion list will show all the user names that start with the given set of letters. When the user selects one of them, presses enter , or hits the "Search" button , all the user names that with the given set of letters will be shown on the data grid, including the users details.



6.3.5 *Adding templates to a selected user:*

By pressing on the button you can add templates to an existing user.

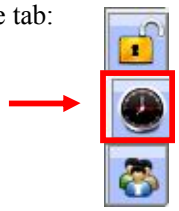
6.4 Opening gate/door:

The system will allow gate opening only if the Relay controller is correctly set.
Make sure your Relay controller is well connected, and correctly defined in system settings. The Relay COM port should be selected on the settings page.
The system will show only the connected and available COM ports.

To open the gate, click the Lock tab. The gate will open.
The gate will be closed after X seconds according to the system settings delay definitions.

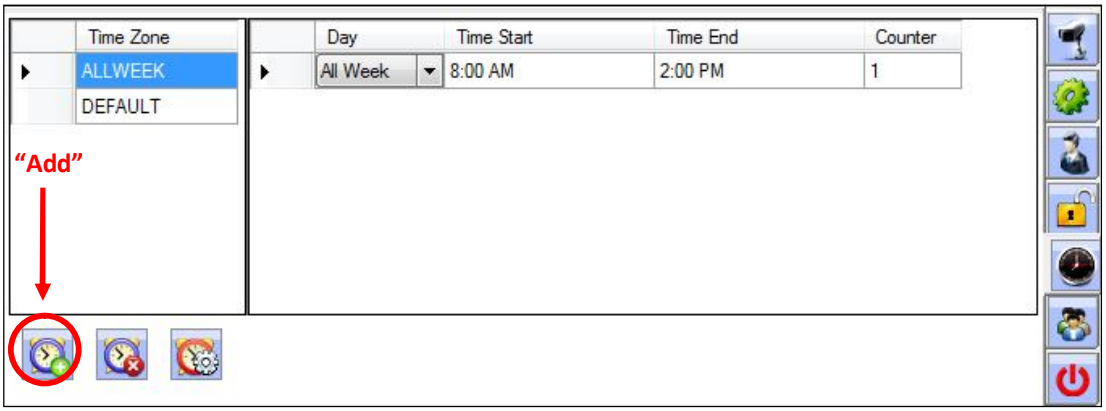
6.5 Timezone Tab:

It is possible to set the working hours of user. To do so, click the timezone tab:

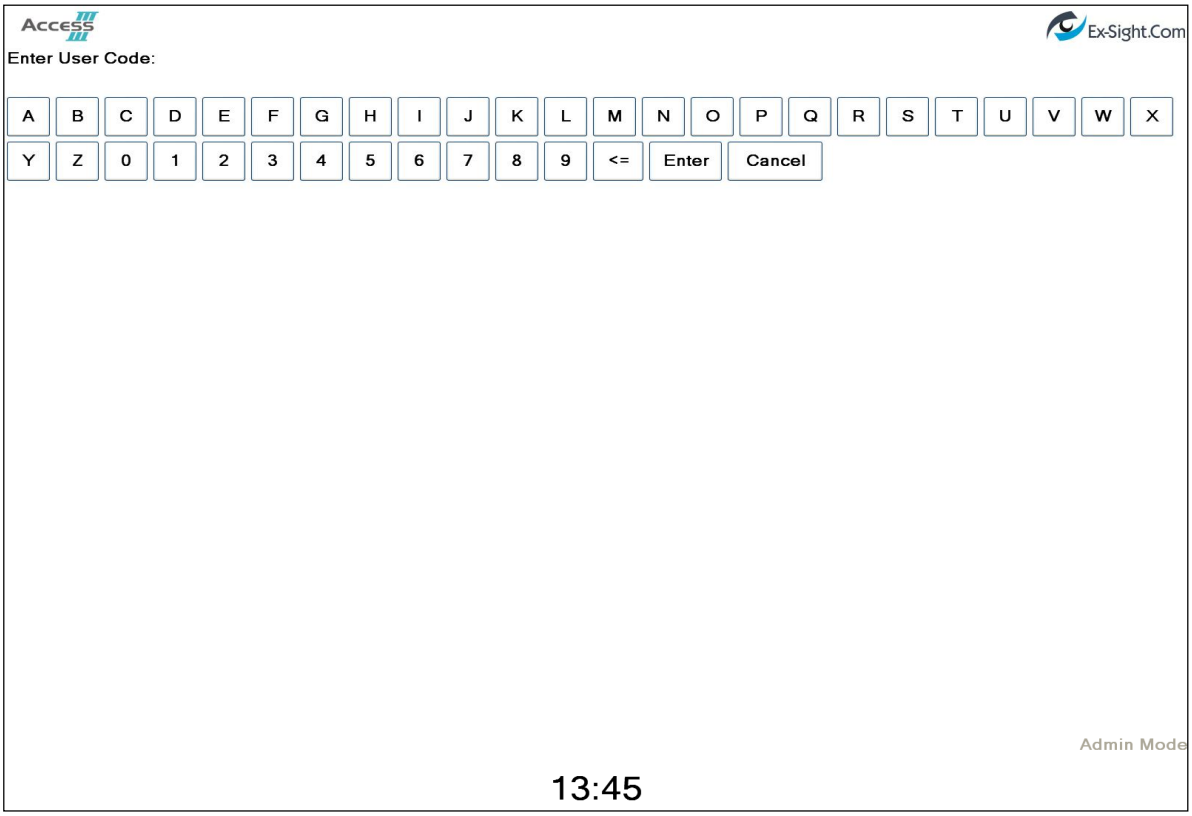


6.5.1 Creating a Primary Time zone:

To create a new primary Time zone click the “Add” icon.

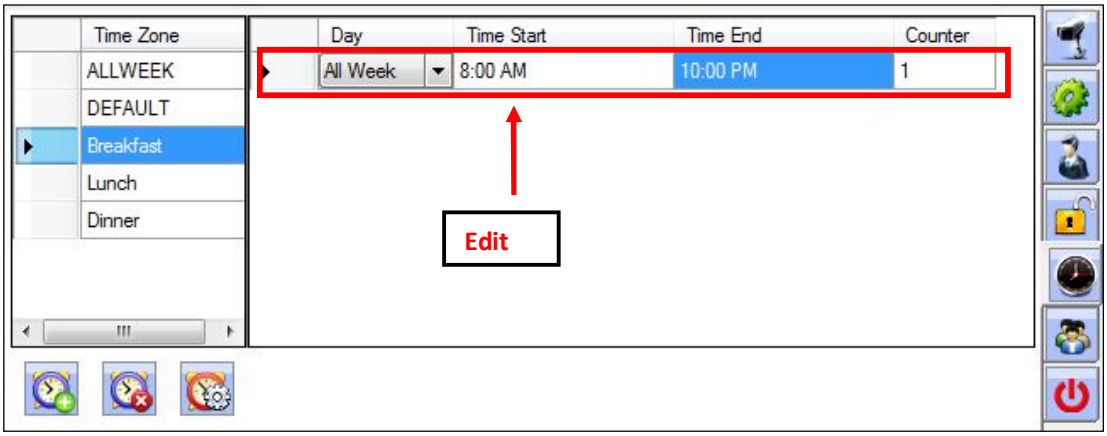


The next window will open:



Enter the new Time Zone name and click “Enter”. The new Time Zone will be saved.

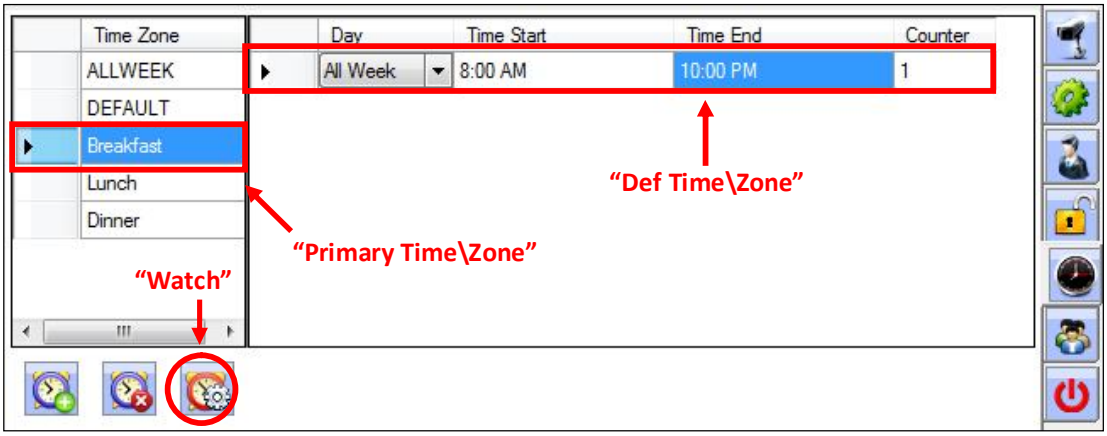
After the new Time zone is saved, you can edit the days of the week or the start/end time. Click the relevant columns and change the values. If the values are invalid, you won't be able to move to the next column.



The "Counter" field represents the number of times a user can access the same time zone per day, per sub-time zone.

6.5.2 *Adding a def Time zone:*

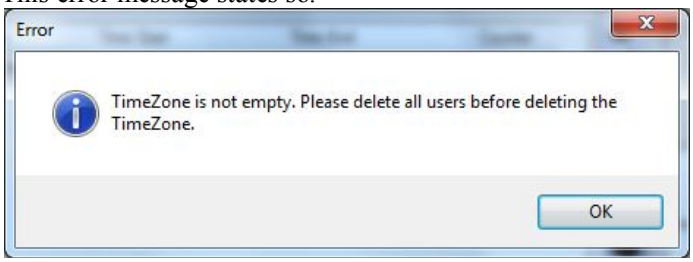
From the list of primary Time zones choose the primary Time zone that you wish to add to a def Time zone to. Click the watch icon.



A new row is added to the current primary Time zone. Click the relevant gap and change the values. If the values are invalid, you won't be able to move to the next gap.

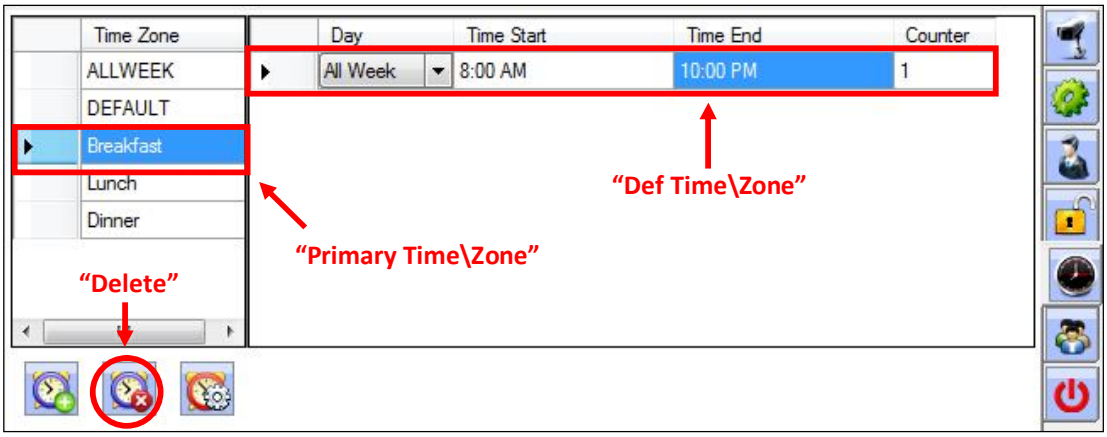
6.5.3 *Deleting Time zone:*

To delete a Primary Time zone, first of all, all the users need to be assigned out of the Timezone. This error message states so.

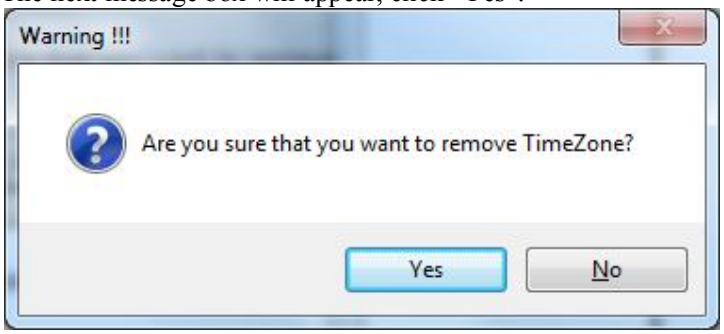


Go to the User Management tab and remove all the users assigned to this Time zone by assigning the users to a different Time zone. Only if the Time zone is empty, it can be deleted.

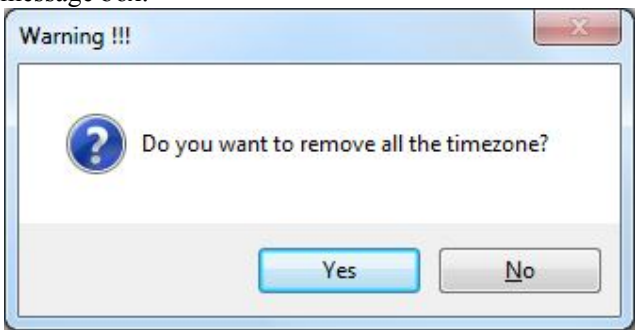
Click the Time zone tab. Choose the Time zone to be deleted by clicking it, and choose the def Time zone. Click the "Delete icon.



The next message box will appear, click "Yes".

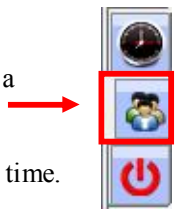


If you wish to delete only the def Time zone and not the whole Time zone, click "No" on the next message box:



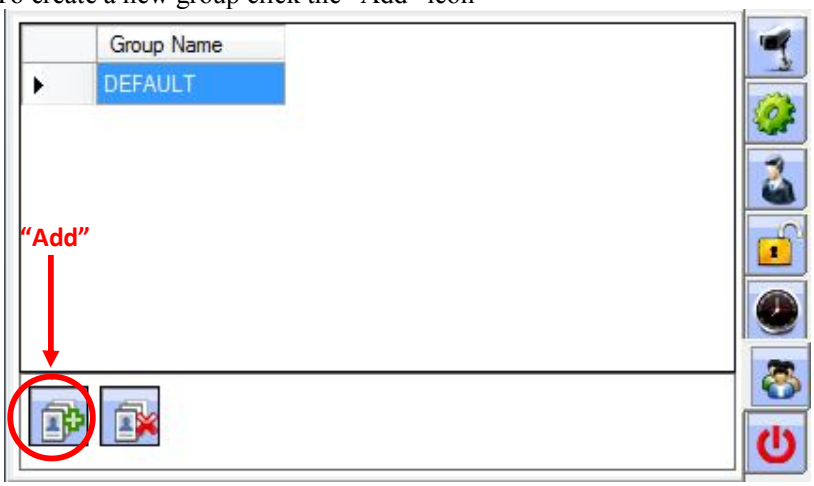
6.6 *Group Tab:*

To configure groups click on the groups tab(as shown on the right).
It is possible for a number of people (as a group) to open the door. If you enter these users into a group and enable the group option under the settings tab:
Group Settings -> Allow Group -> Enable
The door will open if all the users in the group are present within the camera frame at the same time.
The detection delay can be set under: Group Settings -> Group Delay.

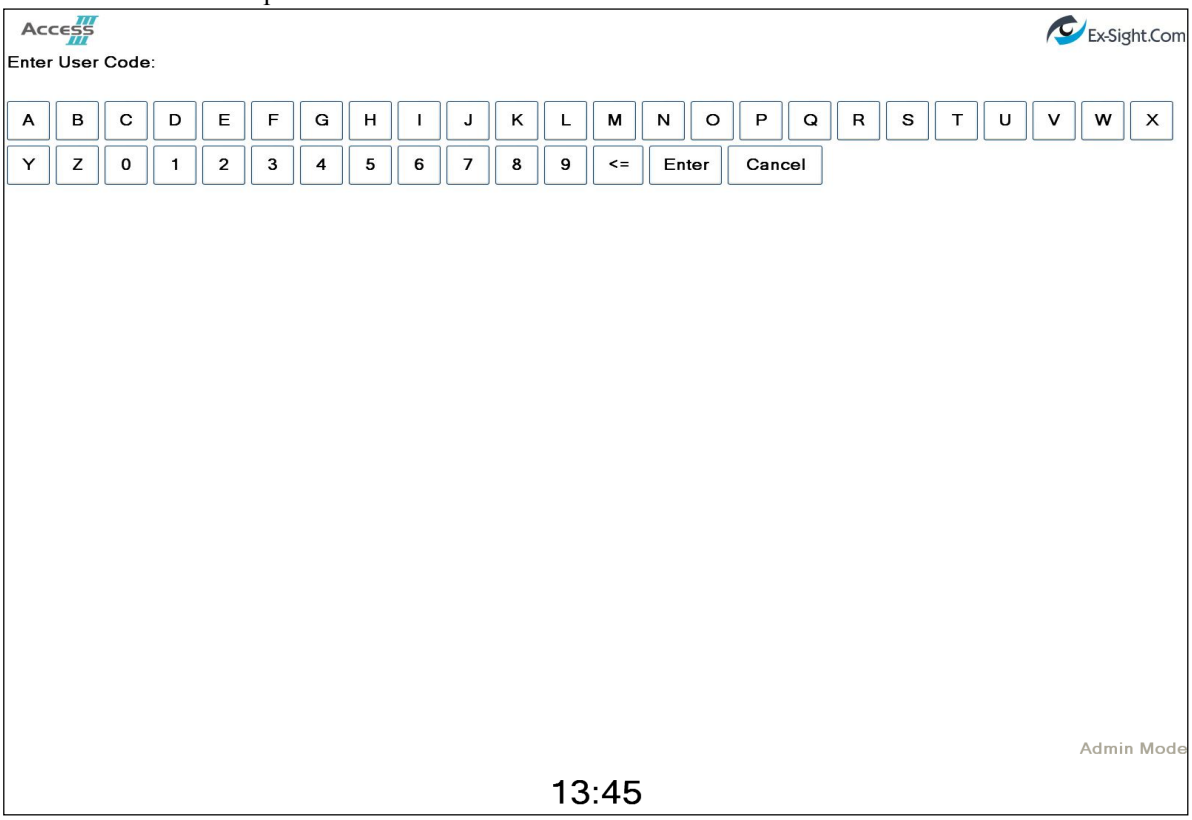


6.6.1 *Creating a group:*

To create a new group click the "Add" icon

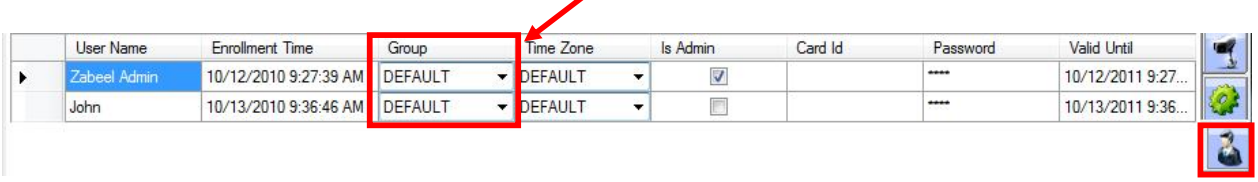


The next window will open:



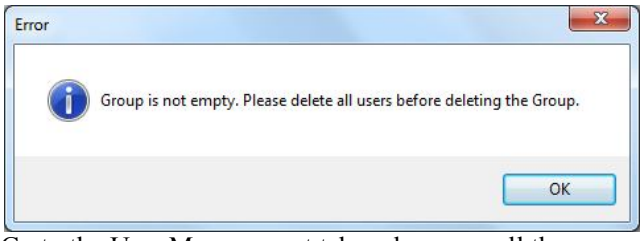
Enter the new group name and click "Enter". The new group is saved.

To add a user to the group, click the users tab and on each user that should be added to this group, change the group name to the new group name created:



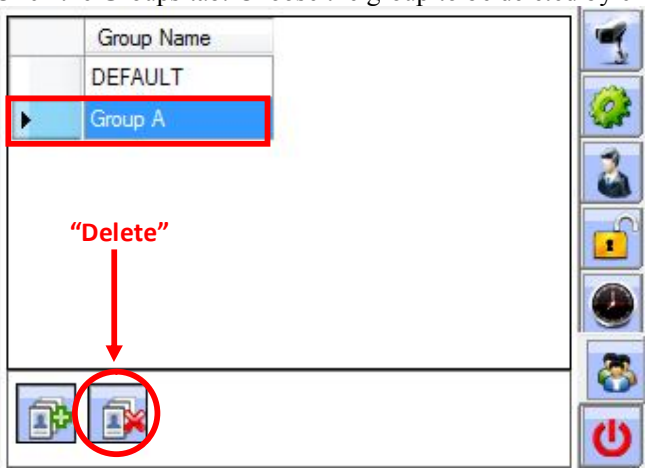
6.6.2 *Deleting a group:*

To delete a group, first of all, all the users need to be assigned out of the group. This error message states so.

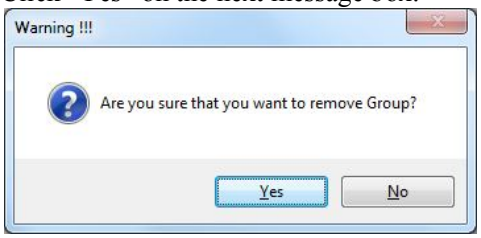


Go to the User Management tab and remove all the users assigned to this group by assigning the users to a different group. Only if the group is empty, it can be deleted.

Click the Groups tab. Choose the group to be deleted by clicking on it and clicking the “Delete” icon.



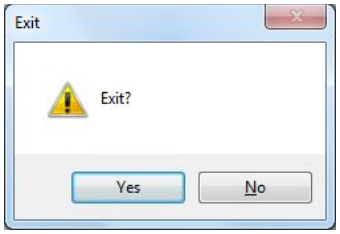
Click “Yes” on the next message box:



6.7 *Shutdown Tab:*

Click the Shutdown button to close the application:

And click “Yes” on the next message box

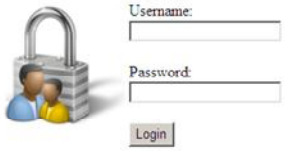


The application will then close.

AccessIII Web Interface:

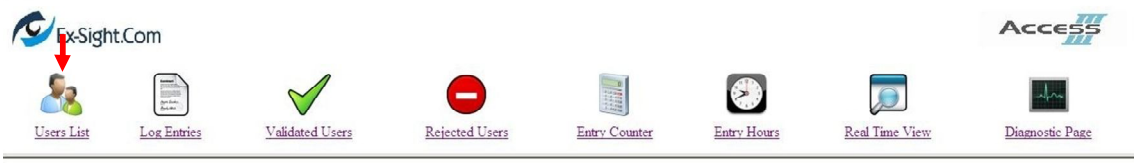
In order to access the AccessIII Web Interface, open an internet explorer window. At the address field enter distant machine's IP address in the net format //ip_address.
Enter your username and password and click “Login” at the next window.

The user name and password should match the Administrator user name and password on the AccessIII software located on the distant machine.



6.8 *Users List:*

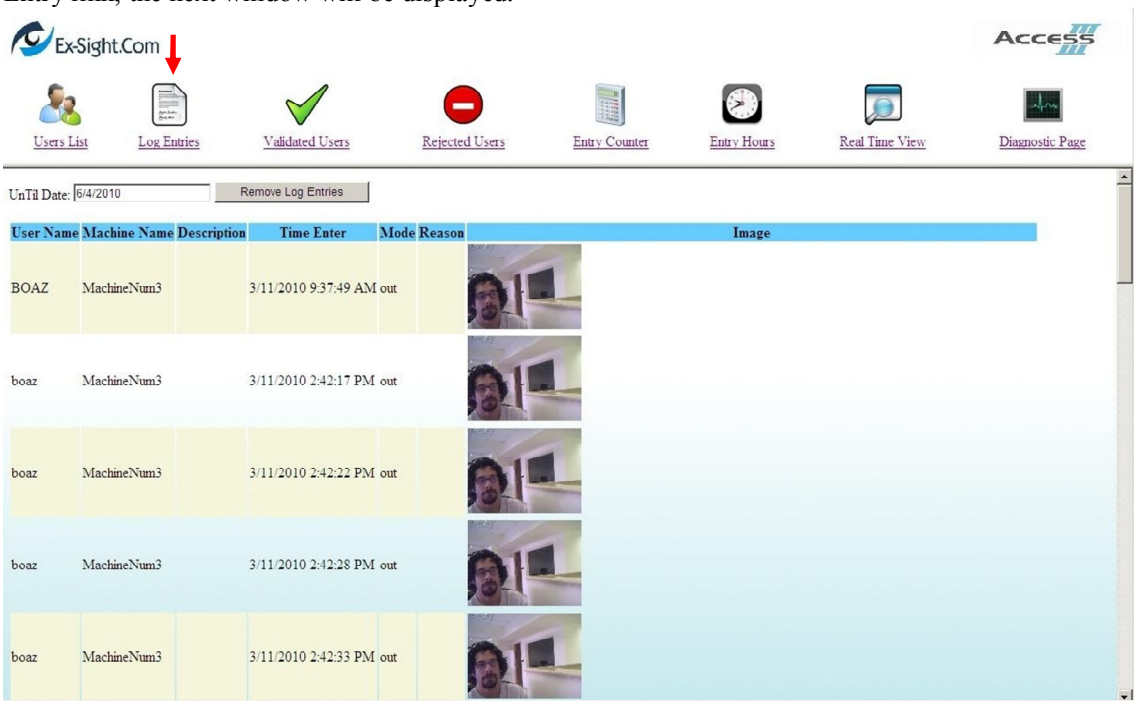
Click the Users List link, to display all the existing users in the system.



User Name	Enrol Time	Group Name	Time Zone	Is User Admin	Card Id	Valid Until	Image
BOAZ	3/11/2010 9:37:03 AM	DEFAULT	DEFAULT	True		3/11/2011 9:37:03 AM	
maya	4/6/2010 2:45:31 PM	DEFAULT	DEFAULT	False		4/6/2011 2:45:31 PM	

6.9 *Log Entry:*

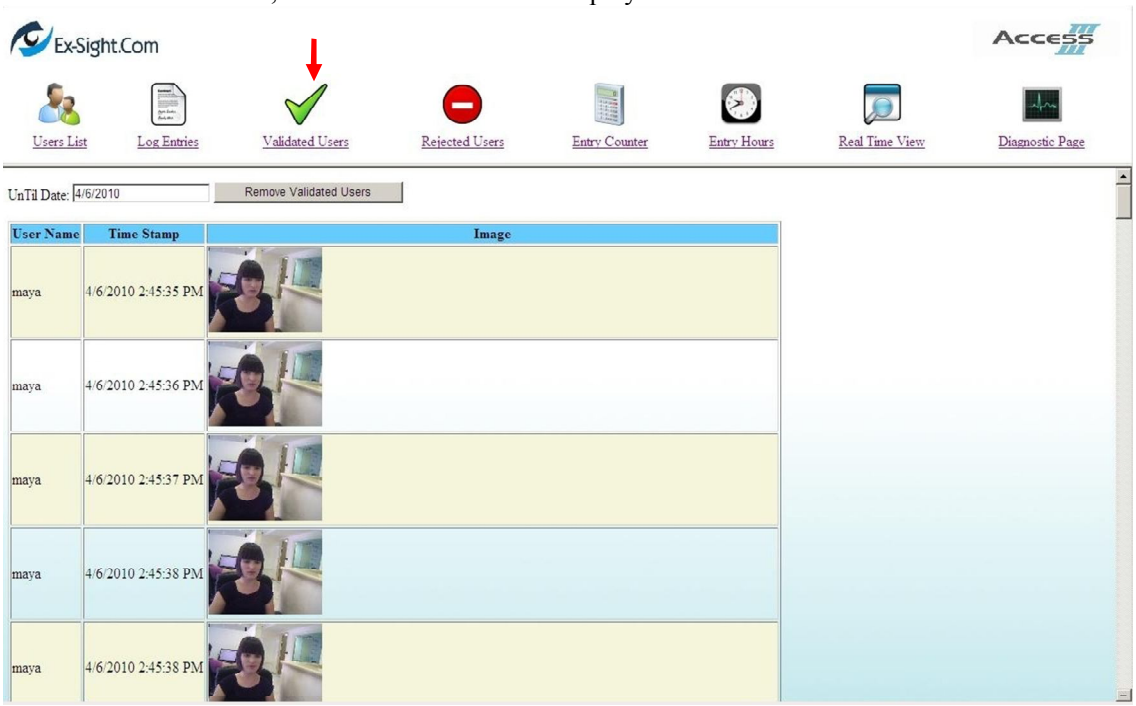
It is possible to view the log entries of all/specific users, filtered by specific dates. By clicking the Log Entry link, the next window will be displayed.



Enter the dates for data retrieval. Select the wanted user to be viewed.
If no user selecting has been done, the system will locate all users' images for the specified dates.
Click “Search”. The list of the relevant images will be displayed.

6.10 Validated Users:

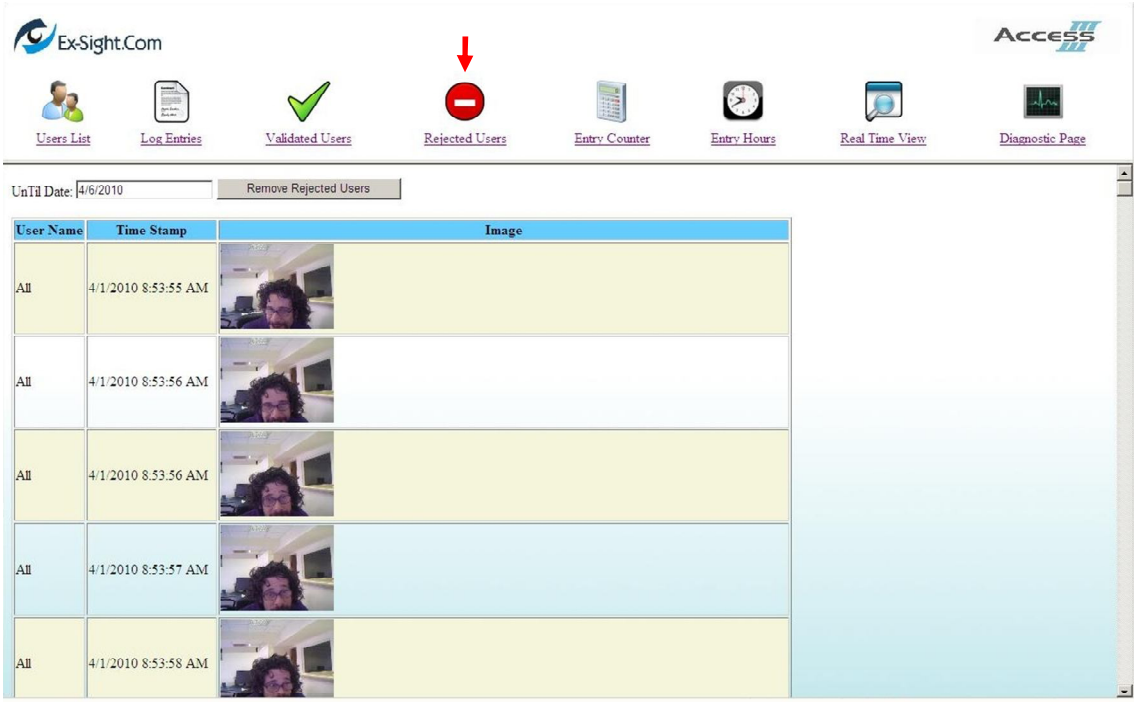
It is possible to view the data & images of the validated users, filtered by specific dates. By clicking the Validated Users link, the next window will be displayed.



Enter the dates for data retrieval. Select the wanted user to be viewed.
If no user selecting has been done, the system will locate all users' images for the specified dates.
Click "Search". The list of the relevant images will be displayed.

6.11 Rejected Users:

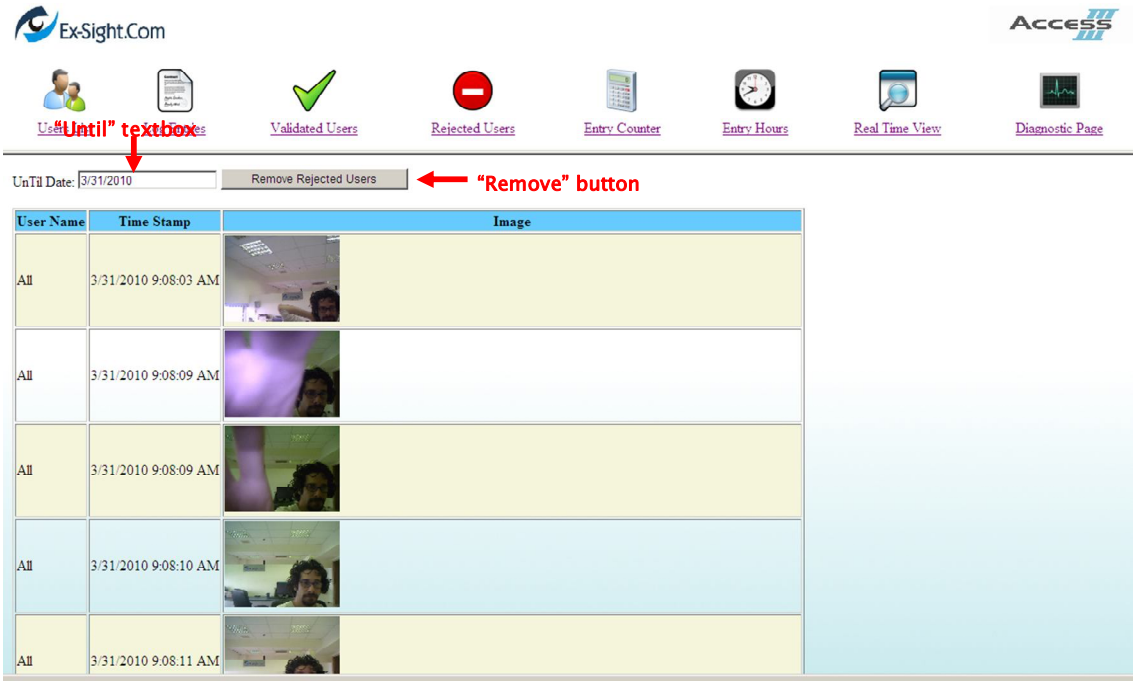
It is possible to view the data and images of the rejected users, filtered by specific dates. By clicking the Rejected Users link, the next window will be displayed.



Enter the dates for data retrieval. Select the wanted user to be viewed.
If no user selecting has been done, the system will locate all users' images for the specified dates.
Click "Search". The list of the relevant images will be displayed.

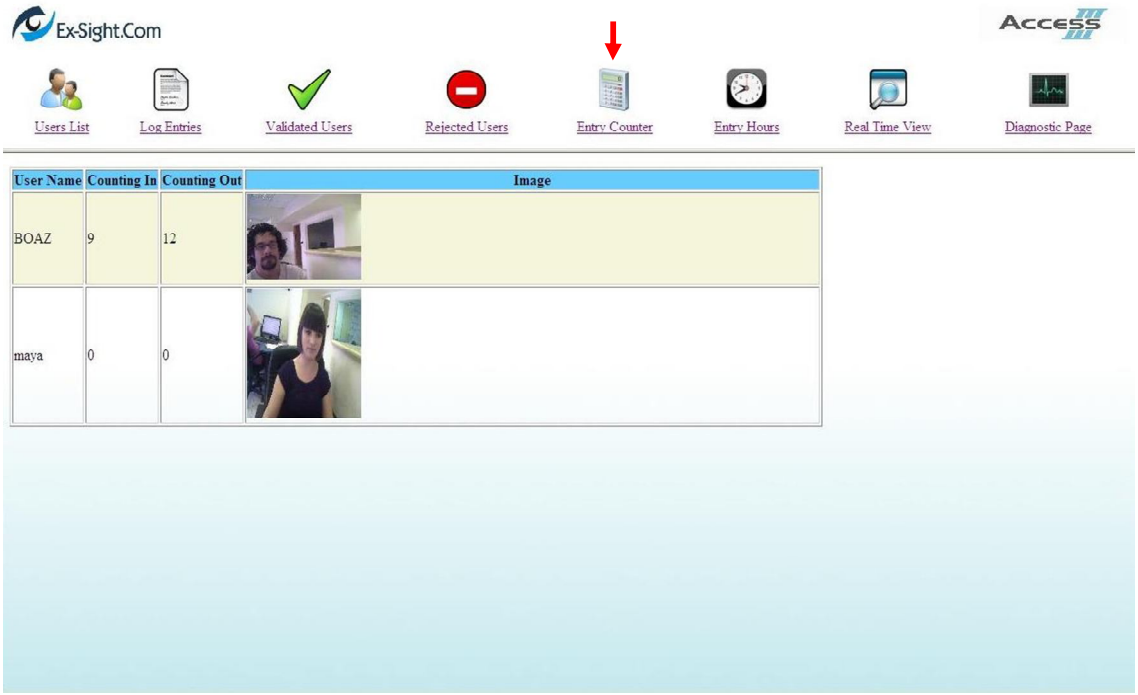
Remove Rows From Database:

It is possible to remove rows in the: "Log Entry", "Validated Users" and "Rejected Users" links. This option reveals after clicking the "Search" button. By entering an "Until" date and clicking "Remove", all the entries until the specified date will be removed from the database.



6.12 *Entry counter:*

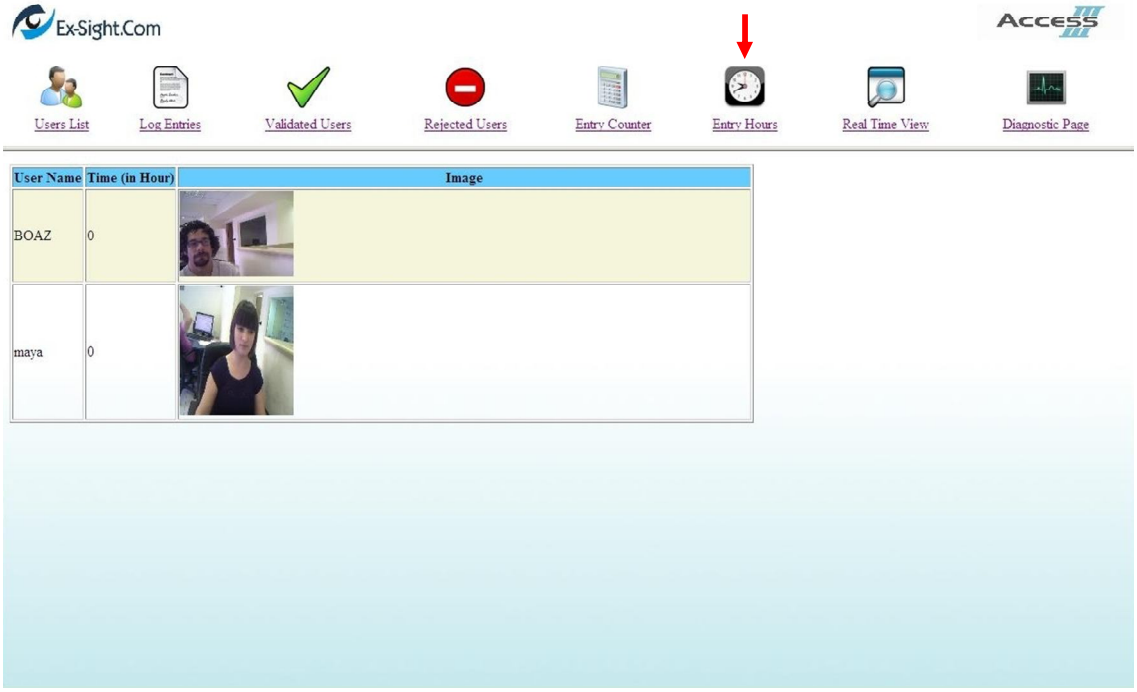
Entry counter will function only if in the system settings, counting feature is enabled. It is possible to view Entry Counter for a specific user or for all users. By clicking the Entry counter link, the next window will be displayed.



Enter the dates for data retrieval. Select the wanted user to be viewed.
If no user selecting has been done, the system will locate all users Entry Counters for the specified dates. By clicking "Search", the relevant list will be displayed.

6.13 Entry Hours: Calculating working hours

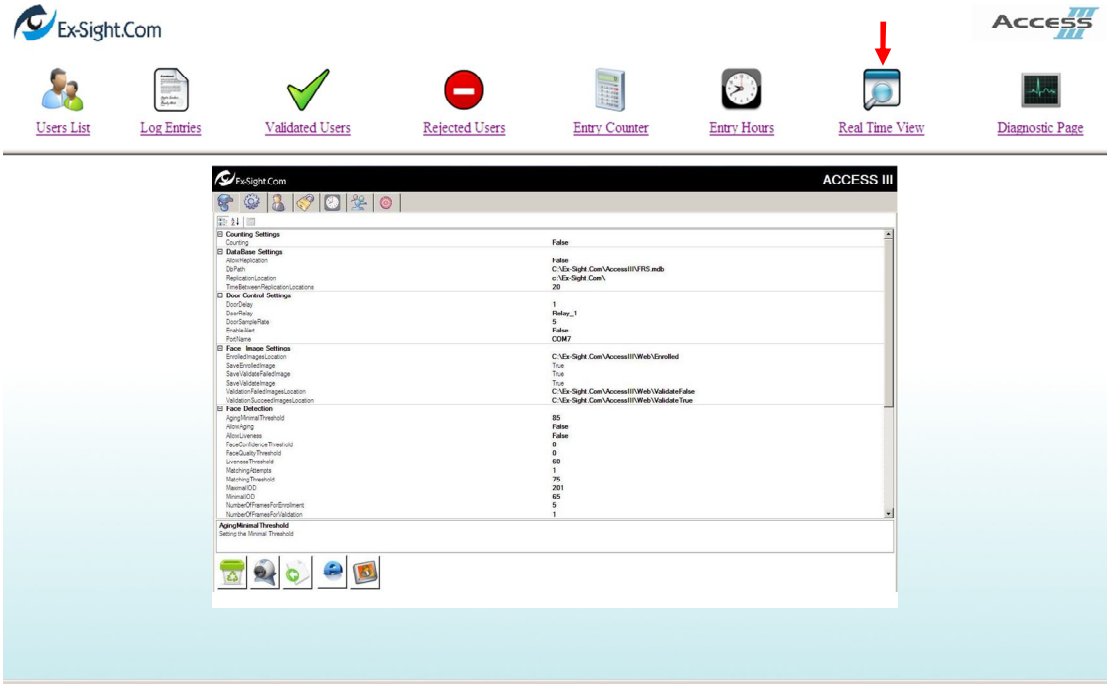
It is possible to calculate total entry hours (calculate number of hours between In and out entries). By clicking the Entry Hours link, the next window shall be displayed:



Enter the dates for data retrieval. Select the wanted user to be viewed.
If no user selecting has been done, the system will locate all users' Entry Hours for the specified dates.
Click "Search". The relevant list will be displayed.

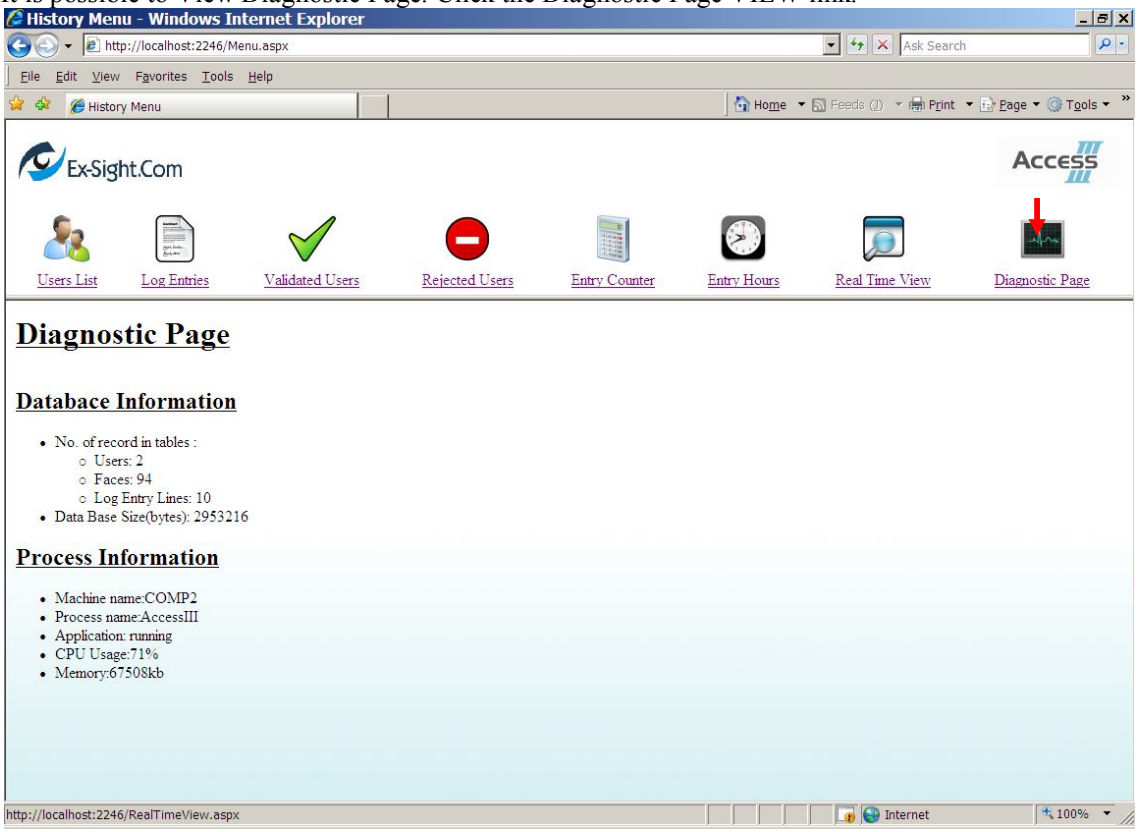
6.14 Realtime View:

It is possible to remotely monitor the AccessIII application. Click the REALTIME VIEW link to do so. The next window will be displayed, showing what goes on the remote application.



6.15 Diagnostic Page:

It is possible to View Diagnostic Page. Click the Diagnostic Page VIEW link.



For more information please contact our customer support department at: support@ex-sight.com

Change List:

- One to One mode
  - Users identify by their user code(which can be the RFID card number/magnetic card number)
- Users
  - User search button
  - Add templates to user button
- Settings
  - Remote Control(Added the option of working vs. a remote webservice instead of local DB)
    - Allow Remote DB mode
    - Interval Time Out
    - Mode Action
    - Remote IP Address
    - Remote Validate Mode
    - Server Timeout